

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Tadashi KOJIMA, et al.

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HEREWITH

FOR: CONTENT MANAGEMENT METHOD, RECORDING AND/OR REPRODUCING APPARATUS, AND
RECORDING MEDIUM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

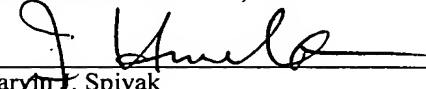
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-348925	November 29, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marylin J. Spivak
Registration No. 24,913
James D. Hamilton
Registration No. 28,421

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年11月29日

出 願 番 号
Application Number:

特願2002-348925

[ST.10/C]:

[JP2002-348925]

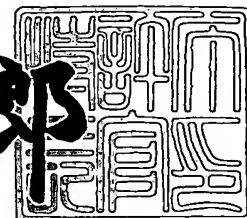
出 願 人
Applicant(s):

株式会社東芝

2003年 6月10日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3045094

【書類名】 特許願

【整理番号】 A000205575

【提出日】 平成14年11月29日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 31/00

【発明の名称】 コンテンツ管理方法、記録再生装置、及び記録媒体

【請求項の数】 14

【発明者】

 【住所又は居所】 東京都青梅市新町3丁目3番地の1 東芝デジタルメディアエンジニアリング株式会社内

 【氏名】 小島 正

【発明者】

 【住所又は居所】 東京都港区芝浦一丁目1番1号 株式会社東芝本社事務所内

 【氏名】 山田 尚志

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 加藤 拓

【発明者】

 【住所又は居所】 神奈川県横浜市磯子区新杉田町8番地 株式会社東芝横浜事業所内

 【氏名】 石原 淳

【発明者】

 【住所又は居所】 東京都青梅市新町3丁目3番地の1 東芝デジタルメディアエンジニアリング株式会社内

 【氏名】 平良 和彦

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ管理方法、記録再生装置、及び記録媒体

【特許請求の範囲】

【請求項 1】

第 1 の鍵でコンテンツデータを暗号化し、
前記第 1 の鍵を予め定められた複数種類の第 2 の鍵で暗号化し、
前記暗号化された第 1 の鍵を第 3 の鍵で多重暗号化し、
前記第 3 の鍵を予め定められた第 4 の鍵で暗号化し、
前記第 1 の鍵で暗号化されたコンテンツデータと、前記予め定められた複数種類の第 2 の鍵で暗号化された第 1 の鍵と、前記暗号化された第 1 の鍵を第 3 の鍵で多重暗号化された第 1 の鍵とを記録媒体に記録し、前記第 4 の鍵で暗号化された第 3 の鍵を前記記録媒体の秘匿領域に記録する、
ことを特徴とするコンテンツ管理方法。

【請求項 2】

複数の第 1 の鍵でコンテンツデータを暗号化し、
前記複数の第 1 の鍵を予め定められた複数種類の第 2 の鍵で暗号化し、
前記暗号化された複数の第 1 の鍵を第 3 の鍵で多重暗号化し、
前記第 3 の鍵を予め定められた一種類以上の第 4 の鍵で暗号化し、
前記第 1 の鍵で暗号化された複数のコンテンツデータと、前記予め定められた複数種類の第 2 の鍵で暗号化された複数の第 1 の鍵と、前記暗号化された第 1 の鍵を第 3 の鍵で多重暗号化された複数の第 1 の鍵とを記録媒体に記録し、前記第 4 の鍵で暗号化された第 3 の鍵を前記記録媒体の秘匿領域に記録する、
ことを特徴とするコンテンツ管理方法。

【請求項 3】

前記第 3 の鍵は、前記複数のコンテンツデータの数に応じて設けられた前記複数の第 1 の鍵の数に応じて複数設けられ、前記暗号化された複数の第 1 の鍵を複数の第 3 の鍵で個別に多重暗号化して記録することを特徴とする請求項 2 記載のコンテンツ管理方法。

【請求項 4】

前記第 2 の鍵で暗号化された第 1 の鍵と、前記第 2 ・ 第 3 の鍵で多重暗号化された第 1 の鍵とは、前記記憶媒体の異なる記録エリアに記録されることを特徴とする請求項 1 乃至 3 記載のいずれかのコンテンツ管理方法。

【請求項 5】

第 1 の鍵でコンテンツデータを暗号化し、前記第 1 の鍵を予め定められた複数種類の第 2 の鍵で暗号化し、前記暗号化された第 1 の鍵を第 3 の鍵で多重暗号化し、前記第 3 の鍵を予め定められた第 4 の鍵で暗号化する暗号化部と、

前記暗号化部でそれぞれ暗号化された、前記第 1 の鍵で暗号化されたコンテンツデータと、前記予め定められた複数種類の第 2 の鍵で暗号化された第 1 の鍵と、前記暗号化された第 1 の鍵を第 3 の鍵で多重暗号化された第 1 の鍵とを記録媒体に記録し、前記第 4 の鍵で暗号化された第 3 の鍵を前記記録媒体の秘匿領域に記録する記録部と、

を具備することを特徴とする記録装置。

【請求項 6】

第 1 の鍵で暗号化されたコンテンツデータと、

予め定められた複数種類の第 2 の鍵で暗号化された前記第 1 の鍵と、

前記暗号化された第 1 の鍵が更に第 3 の鍵で多重暗号化された第 1 の鍵と、がその記憶領域に記録され、

前記第 4 の鍵で暗号化された第 3 の鍵が前記記憶領域内の秘匿領域に記録されていることを特徴とする記録媒体。

【請求項 7】

記録媒体間に移動を許可されたコンテンツデータが格納されたコンテンツデータ源から、第 1 の記録媒体にコンテンツデータを記録する場合は、第 1 の鍵で暗号化されたコンテンツデータと、記録媒体にバインドされた鍵である第 2 の鍵で暗号化された第 1 の鍵と、第 2 ・ 第 3 の鍵で多重暗号化されたコンテンツ移動制御用暗号鍵とを第 1 の記録媒体に記録し、

前記第 1 の記録媒体から第 2 の記録媒体にコンテンツデータを移動させる場合は、前記コンテンツデータを復号後再暗号化して、暗号化コンテンツデータと、前記コンテンツ移動制御用暗号鍵のみを前記第 2 の記録媒体に記録すると共に、

前記第 1 の記録媒体に記録されているコンテンツ移動制御用暗号鍵を消去する、
ことを特徴とするコンテンツ管理方法。

【請求項 8】

前記コンテンツ移動制御用暗号鍵のみが記録された前記第 2 の記録媒体から、
第 3 の記録媒体にコンテンツデータを移動させる場合は、コンテンツデータ復号
後コンテンツデータを再暗号して、暗号化コンテンツデータとコンテンツ移動制
御用暗号鍵を前記第 3 の記録媒体に記録すると共に、前記第 2 の記録媒体のコン
テンツ移動制御用暗号鍵を消去することで、記録媒体間のコンテンツ移動処理を
行うことを特徴とする請求項 7 記載のコンテンツ管理方法。

【請求項 9】

暗号鍵により暗号化されたコンテンツデータと、
前記暗号鍵を複数の鍵で多重暗号化した、前記コンテンツデータの移動を制御
するためのコンテンツ移動制御用暗号鍵と、
が記憶領域に記録された記録媒体。

【請求項 10】

複数のコンテンツデータを複数の第 1 の鍵で個別暗号化し、前記複数の第 1 の
鍵を予め定められた複数種類の第 2 の鍵で暗号化し、前記暗号化された第 1 の鍵
を複数の第 3 の暗号鍵で暗号する場合、

特定の乱数発生器で鍵元データを生成し、前記複数のコンテンツデータを特定
する情報により特定関数を乗算して複数の第 3 の鍵を生成し、これらを複数の暗
号化された第 1 の鍵の多重暗号鍵として、複数の暗号化コンテンツデータと多重
暗号化された第 1 の鍵を記録媒体に記録すると共に、

この記録媒体の秘匿領域に前記乱数発生器で生成された鍵元データを予め定め
られた暗号鍵で暗号化して記録することを特徴とするコンテンツ管理方法。

【請求項 11】

複数のコンテンツデータを複数の第 1 の鍵で個別暗号化し、前記複数の第 1 の
鍵を予め定められた複数種類の第 2 の鍵で暗号化し、前記暗号化された第 1 の鍵
を複数の第 3 の暗号鍵で暗号する場合、特定の乱数発生器で鍵元データを生成し
、コンテンツデータの識別コード、又は、序列番号等で決められる回数で特定関

数を乗算して複数の第 3 の鍵を生成し、これらを複数の暗号化された第 1 の鍵の多重暗号鍵として用いる場合の、

前記複数の暗号化コンテンツデータと、前記多重暗号化された第 1 の鍵と、がその記憶領域に記憶され、

前記乱数発生器で生成された鍵元データが予め定められた暗号鍵で暗号化されて、前記記憶領域内の秘匿領域に記録されていることを特徴とする記録媒体。

【請求項 1 2】

第 1 の鍵でコンテンツデータを暗号化し、前記第 1 の鍵を予め定められた複数種類の第 2 の鍵で暗号化し、暗号化された第 1 の鍵を第 3 の鍵で暗号化し、第 3 の鍵を予め定められた第 4 の鍵で暗号化し、暗号化されたコンテンツデータを記録すると共に、第 2 の鍵で暗号化された第 1 の鍵と第 2 ・第 3 の鍵で多重暗号化された第 1 の鍵を夫々独立ファイルデータとして独立した記録エリアに記録する場合、前記鍵ファイルの先頭、又は、定められた位置に、ファイルの鍵データが、第 2 の鍵で暗号化された第 1 の鍵か、第 2 ・第 3 の鍵で多重暗号化された第 1 の鍵かの識別情報と、夫々相手の鍵ファイルが存在するかの識別情報とを有する暗号化暗号鍵ファイルを更に設けることを特徴とするコンテンツ管理方法。

【請求項 1 3】

第 1 の鍵で暗号化されたコンテンツデータと、
前記予め定められた複数種類の第 2 の鍵で暗号化された前記第 1 の鍵と、
前記前記暗号化された第 1 の鍵が第 3 の鍵で多重暗号化された多重暗号鍵と、
がそれぞれ、独立したファイルデータとして、独立した記録エリアに記録されており、

更に、前記ファイルの鍵データが、第 2 の鍵で暗号化された第 1 の鍵か、前記多重暗号鍵かの識別情報と、夫々相手の鍵ファイルが存在するかの識別情報とを有する暗号鍵ファイルが、前記独立した記録エリアの鍵ファイルの先頭又は定められた位置に更に記録されていることを特徴とする情報記録媒体。

【請求項 1 4】

第 1 の鍵で暗号化されたコンテンツデータと、予め定められた複数種類の第 2 の鍵で暗号化された前記第 1 の鍵と、前記暗号化された第 1 の鍵が更に第 3 の鍵

で多重暗号化された第 1 の鍵と、がその記憶領域に記録され、前記第 4 の鍵で暗号化された第 3 の鍵が前記記憶領域内の秘匿領域に記録されていることを特徴とする第 1 の記録媒体、及び、

前記暗号化されたコンテンツデータと、前記暗号化された第 1 の鍵が更に第 3 の鍵で多重暗号化された第 1 の鍵と、がその記憶領域に記録され、前記第 4 の鍵で暗号化された第 3 の鍵が前記記憶領域内の秘匿領域に記録されていることを特徴とする第 2 の記録媒体の再生方法において、

前記第 1 の記録媒体においては、前記第 2 の鍵で暗号化された第 1 の鍵を読み出し、予め定められた複数種類の第 2 の鍵で暗号化された第 1 の鍵を復号し、暗号化されたコンテンツデータを読み出して前記復号された第 1 の鍵でコンテンツデータを復号処理することで再生し、

前記第 2 の記録媒体においては、前記秘匿領域から暗号化された第 3 の鍵を読み出し、予め定められた複数種類の第 4 の鍵で暗号化された第 3 の鍵を復号し、前記多重暗号化された第 2 の鍵を読み出し前記第 3 の鍵で復号して第 2 の鍵で暗号化された第 1 の鍵を検出し、予め定められた複数種類の第 2 の鍵で暗号化された第 1 の鍵を復号し、暗号化されたコンテンツデータを前記復号された第 1 の鍵でコンテンツデータを復号処理することで再生する、

ことを特徴とするコンテンツ管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツデータを管理するコンテンツ管理方法及びこれを用いた記録再生装置と、これによりコンテンツデータ等が記録された記録媒体に関し、特に、無制限な違法コピーを防止する一方で、コンテンツデータの一定の移動を可能とするコンテンツ管理方法、記録再生装置、及びこれの記録媒体に関する。

【0002】

【従来の技術】

従来、デジタル化された情報（例えば、文書、音声、画像、プログラムなど）を記録する媒体として、音声や画像の記録媒体ではコンパクトディスクやレーザ

ディスクがある。又、コンピュータなどのプログラムやデータの記録媒体には、フロッピーディスクやハードディスクがある。又、これら記録媒体に加えて、大容量記録媒体であるDVD (Digital Versatile Disk) が開発されている。

【0003】

このような種々のデジタル記録媒体において、記録する時にそのままデジタルデータ（圧縮や符号化等されデコード可能なもの含む）を記録している為、記録されたデータを他の媒体にコピーすることは、例えば音質や画質の損失なしに、かつ容易にコピーすることができる。従って、これらのデジタル記録媒体では、複製を大量に作り出しことができ、著作権の侵害等の問題がある。

【0004】

これに応じて、従来技術のコンテンツ暗号化・復号化方法として、コンテンツの違法コピー防止を課題として、再生専用のDVD-videoディスクについて、CSS (Content Scramble System) と呼ばれる著作権保護システムが導入されている（例えば、特許文献1参照）。

【0005】

【特許文献1】

特開平09-136709号公報。

【0006】

【発明が解決しようとする課題】

しかし、上記した従来装置では、違法コピーを防止し著作権保護しながらコンテンツ移動を行う一方で、同時に、汎用機である従来の再生装置によりコンテンツの再生を行うということができない。すなわち、コンテンツデータの移動を適宜行いながら、しかも、従来装置による再生も行うというユーザの利便性を確保することができないという問題がある。

【0007】

本発明は、コンテンツの拡散を防止しながらコンテンツの移動を可能にする一方で、従来の汎用装置での最小限の再生互換性も保証するコンテンツ管理方法と記録再生装置及び記録媒体を提供することを目的とする。

【0008】

【課題を解決するための手段】

本発明は、上記課題を解決するべく、第1の鍵（TK）でコンテンツデータを暗号化し、前記第1の鍵を予め定められた複数種類の第2の鍵（MUK）で暗号化し、前記暗号化された第1の鍵（Enc-TK）を第3の鍵（MM）で多重暗号化し、前記第3の鍵を予め定められた第4の鍵（MMK）で暗号化し、前記第1の鍵で暗号化されたコンテンツデータ（Enc-Contents）と、前記予め定められた複数種類の第2の鍵で暗号化された第1の鍵（Enc-TK）と、前記暗号化された第1の鍵（Enc-TK）を第3の鍵（MM）で多重暗号化された第1の鍵（Enc2-TK）とを記録媒体に記録し、前記第4の鍵で暗号化された第3の鍵（Enc-MM）を前記記録媒体の秘匿領域に記録する、ことを特徴とするコンテンツ管理方法である。

【0009】

本発明は、上記したように、コンテンツ移動制御用暗号鍵である移動キー（Move-Key）であり、コンテンツの暗号鍵を第2・第3の鍵で多重暗号化したタイトル鍵である、多重暗号化された第1の鍵（Enc2-TK）を記録媒体に記録することで、コンテンツ移動を一定の制約の中で可能とする。その一方で、移動キー（Move-Key）に対応する専用機ではなく、従来の汎用機でもコンテンツを再生可能とするべく、タイトル鍵（TK）を一度だけ第2の鍵（MKB, M-ID）で暗号化した、メディアバインドされたタイトル鍵である媒体キー（Enc-TK）も、異なる領域に記録する。これにより、媒体キー（Enc-TK）によって汎用機での再生を可能とすると共に、移動キー（Move-Key）によって、コンテンツデータの拡散を防止しつつコンテンツ移動を可能とするものである。

本発明は更に、記録媒体間に移動を許可されたコンテンツデータが格納されたコンテンツデータ源（S）から、第1の記録媒体（D1）にコンテンツデータを記録する場合は、第1の鍵（TK）で暗号化されたコンテンツデータ（Enc-Contents）と、記録媒体にバインドされたコンテンツ暗号鍵（MB-KEY）である第2の鍵で暗号化された第1の鍵（Enc-TK）と、第2・第3の鍵で多重暗号化されたコンテンツ移動制御用暗号鍵（Enc2-TK）と、を第1の記

録媒体（D1）に記録し（フロー1）、前記第1の記録媒体（D1）から第2の記録媒体（D2）にコンテンツデータを移動させる場合は、前記コンテンツデータを復号後再暗号化して、暗号化コンテンツデータと、前記コンテンツ移動制御用暗号鍵のみを第2の記録媒体に記録すると共に、前記第1の記録媒体に記録されているコンテンツ移動制御用暗号鍵を消去する（フロー2）ことを特徴とするコンテンツ管理方法である。

【0010】

本発明に係るコンテンツ管理方法は、コンテンツの移動方法を特定するものであり、上述した二つのキー、汎用機再生用の媒体キー（Enc-TK）と、コンテンツ移動用の移動キー（Move-Key）について、コンテンツデータ源（S）から第1のディスク（D1）へのコンテンツデータの記録においては、二つの鍵を記録して、今後のコンテンツの移動を可能とすると共に、専用機以外の汎用機による再生にも同時に対応させるものである。第1のディスク（D1）から第2のディスク（D2）へのコンテンツデータの移動に際しては、第1のディスク（D1）から移動キー（Move-Key）を削除し、汎用機再生用の媒体キー（Enc-TK）のみを残すものである。これにより、以降の移動は行うことができなくなり、更に、汎用機の再生は今後とも行うことができる。第2のディスクへのコンテンツデータの移動においては、移動キー（Move-Key）のみが記録されるため、専用機のみで再生が可能となり、更に、第3以降のディスク等への移動を今後とも続けることができる。

【0011】

本発明に係るコンテンツ管理方法は、上述した最初のディスクへの記録方法やその後の移動方法によって、コンテンツデータの再生や移動を可能とするものであり、コンテンツデータの拡散を防止しながらも、コンテンツデータの移動を可能とし、更に、専用機だけではなく従来の汎用機においても再生することができるコンテンツ管理方法、記録再生装置、及び記録媒体を提供するものである。

【0012】

【発明の実施の形態】

以下、図面を参照して、本発明に係るコンテンツ管理方法、記録再生装置、及

び記録媒体について詳細に説明する。図 1 は、本発明に係るコンテンツ管理方法による暗号化の一例を示すブロック図、図 2 及び図 3 は、暗号化されたコンテンツの一般的な方法による復号の一例を示すブロック図、図 4 は、暗号化されたコンテンツを記録した記録媒体の一例、図 5 は、本発明に係るコンテンツ管理方法による移動キー (Move-Key: Enc2-TK) と媒体キー (MB-Key: Enc-TK) の移動の一例を示す説明図である。

【 0 0 1 3 】

＜本発明に係るコンテンツ管理方法の概要＞

初めに、図面を用いて、本発明に係るコンテンツ管理方法の概要として、暗号化方法とその復号方法を以下に説明する。本発明に係るコンテンツ管理方法においては、コンテンツデータの移動を保証する移動キー (Move-Key: Enc2-TK) と、従来の汎用機 (例えば光ディスク装置等) による再生装置でも再生することを保証する媒体キー (MB-Key: Enc-TK) とを暗号化コンテンツデータと共に記録媒体へと記録することを特徴としている。

(暗号化)

本発明に係るコンテンツ管理方法におけるコンテンツデータの暗号化・記録方法は、図 1 において、AVエンコーダモジュール M1 の働きと、ドライブ V1 の働きにより説明することができる。図 1 の AVエンコーダモジュール M1 において、映像 (V) 音声 (A) 信号は AVエンコーダ 12 で DVDフォーマットにエンコードされ、デジタルデータ 11 と共にセレクタ 13 で選択された後に、スクランブル回路 14 でタイトル鍵 (TK) によりスクランブル (暗号化) 処理され、ディスク D に (Enc-Contents) として記録される。

【 0 0 1 4 】

この時のタイトル鍵 (TK) は、乱数発生器 18 で生成される。暗号化鍵 TK は、暗号化回路 20 で暗号鍵 (MUK) によって暗号化されて暗号化タイトル鍵 (Enc-TK) となる。ここで、タイトル鍵 (TK) を暗号化した暗号鍵 (MUK) は、デバイス鍵 K1 (DvK116) を、記録メディアから読み出された (MKB) データにより MKB処理 17 で MKB処理してメディア鍵 (MMK) を生成し、これを更に記録メディアから読み出されたメディア固有情報 (M-I

D)により、MID処理19でMID処理して生成することにより得られるものである。

更に、暗号化されたタイトル鍵 (Enc-TK) を秘匿鍵 (MM) で多重暗号化して、多重暗号化タイトル鍵 (Enc2-TK) を生成し、暗号化タイトル鍵 (Enc-TK) と同様に、セクタ27へと供給する。

【0015】

ここで、秘匿鍵 (MM) は、乱数発生器24により供給されるものである。ドライブV1固有のデバイス鍵 (DvK2) を、記録媒体から与えられたMKBによりMKB処理23でMKB処理を行い、得られた暗号鍵 (MMK) によって、この秘匿鍵 (MM) は暗号化され、暗号化暗号鍵 (Enc-MM) が得られる。

このように得られた暗号化されたコンテンツデータ (Enc-Contents) と、暗号鍵 (MUK) で暗号化されたタイトル鍵 (Enc-TK) (=媒体キー (MB-Key)) と、第2・第3の鍵で多重暗号化されたタイトル鍵 (Enc2-TK) (=移動キー (Move-Key)) とは、それぞれ、光ディスクDの記憶領域に記録される。更に、先の暗号化された第3の鍵 (Enc-MM) を光ディスクDの秘匿領域に記録する。これらの信号の光ディスクDへの記録の一例を、図4に示す。

【0016】

すなわち、ここで、本発明に係るコンテンツ管理方法の特徴である、移動キー (Move-Key; Enc2-TK) と媒体キー (MB-Key; Enc-TK) との両方 (コンテンツ移動後は、一方) が、記録処理制御部であるR-Controller 15からの制御信号に応じたセクタ27を介して光ディスクDへと記録される。

【0017】

ここで、光ディスク記録メディアに記録された情報を他の再生装置での再生互換を実現するため、複数のデバイス鍵 (Dvk) でも同一の鍵情報 (MK) が生成され、更に、メディア固有情報 (M-ID) によってメディアバインドが行われることで、他のメディアに丸ごとコピーされることを防止している。

【0018】

又、二つの暗号鍵、移動キー (Move-Key; Enc2-TK) と媒体キー (MB-Key; Enc-TK) とが、後に詳述するように、コンテンツのコピーや移動の際には、選択的に光ディスクDに記録されることにより、一定条件下での汎用機での再生や、限定的なコンテンツデータの移動処理を可能にしている。

【0019】

(二つの再生方法)

このようにして図4が示すように暗号化されたコンテンツデータと、暗号化された鍵情報とが記録された光ディスクDは、以下に示すように、少なくとも媒体キー (MB-Key; Enc-TK) が記録された光ディスクDは、従来の汎用的な光ディスク再生装置で再生できる。更に、移動キー (Move-Key; Enc2-TK) のみが記録された光ディスクDは、本発明に係るコンテンツ管理方法が行われる光ディスク再生装置のみで再生される。

【0020】

すなわち、図2は、従来の汎用機である再生装置で本発明に係る媒体キー (MB-Key; Enc-TK) のみを用いて行われる復号処理を示す図である。この図において、少なくとも媒体キー (MB-Key; Enc-TK) が記録された光ディスクDは、ドライブV2を介して、メディアに予め記録されているメディア鍵ブロック情報 (MKB) 及びメディア固有情報 (M-ID) と、媒体キー (MB-Key; Enc-TK) とが、バス認証21を介してAVデコーダモジュールM2へと供給される。更に、暗号化されたコンテンツデータ (Enc-Contents) がAVデコーダモジュールM2へと供給される。

【0021】

この暗号化コンテンツデータ (Enc-Contents) は、デスクランブル29でタイトル鍵 (TK) によってデスクランブル (復号化) 処理され、AVデコーダ30へと供給されて再生される。ここで、タイトル鍵 (TK) は、暗号化タイトル鍵 (Enc-TK) がディスクDから読み出され、復号部28に送られて、暗号鍵 (MUK) で復号されることにより得られる。又、暗号鍵 (MUK) は、記録側と同様に、メディア鍵ブロック情報 (MKB)、メディア固有情報 (M-ID

D) によるMKB処理17、MID処理19により取得されるものである。

これにより、本発明に係るコンテンツデータ管理方法による処理を行わない、従来の光ディスク再生装置等でも、媒体キー (M B - K e y ; E n c - T K) が記録された光ディスクDのコンテンツデータは、再生することが可能となる。

一方、図3に示すように、移動キー (M o v e - K e y ; E n c 2 - T K) のみしか与えられていない光ディスクDにおいては、本発明に係るコンテンツデータ管理方法による処理を行うことで、初めて再生することができるものである。

すなわち、光ディスク装置から、メディア鍵ブロック情報 (MKB) と暗号化タイトル鍵 (E n c - M M) と多重暗号化タイトル鍵 (E n c 2 - T K) と暗号化コンテンツ (E n c - C o n t e n t s) とが与えられたドライブV1は、ドライブV1固有のデバイス鍵 (D v K 2) でMKB処理23することにより得られる鍵 (M M K) により復号部31により復号して秘匿鍵 (M M) を得、これにより、多重暗号化されたタイトル鍵 (E n c 2 - T K) を暗号化タイトル鍵 (E n c - T K) へと復号し、バス認証21を経てモジュールM2へと供給する。

【0022】

モジュールM2では、モジュールM2固有のデバイス鍵 (D v K) をメディア鍵ブロック情報 (MKB) によりMKB処理17し、メディア固有情報 (M - I D) によりMID処理19して得た暗号鍵 (M U K) によって、暗号化タイトル鍵 (E n c - T K) を復号部28で復号してタイトル鍵 (T K) を得る。

【0023】

このタイトル鍵 (T K) を用いることで、暗号化されたコンテンツデータ (E n c - C o n t e n t s) をデスクランブル部29で復号することにより、コンテンツデータをAVデコーダ30へと供給することができる。

このように、移動キー (M o v e - K e y ; E n c 2 - T K) のみを与えた光ディスクDにおいては、本発明に係るコンテンツデータ管理方法による処理を行う光ディスク記録再生装置のみで再生や後述する移動が可能となるものである。

(本発明に係るコンテンツデータ管理方法によるコンテンツ移動)

次に、本発明に係るコンテンツデータ管理方法によるコンテンツデータの移動方法の一例について、その概要を説明する。図5において、本発明に係るコンテ

ンツデータ管理方法では、移動キー (Move-Key: すなわち、Enc2-TK) と媒体キー (MB-Key: すなわち、Enc-TK) との二種類のキーを用いて、これを適宜、記録媒体に記録させることで、再生やコピー、移動について制限を与えることができる。すなわち、本発明に係るコンテンツデータ管理方法によれば、光ディスク等の記録メディアは、「媒体キー (MB-Key) と移動キー (Move-Key)」 「媒体キー (MB-Key) のみ」 「移動キー (Move-Key) のみ」 の三種類が存在する。ここでは、コンテンツデータ等については説明を省略し、この二つの媒体キーと移動キーについてだけ概要説明する。

図5において、初めに、コピー制限されたソースコンテンツSは、最初のディスクD1 (記録媒体) に対して、媒体キー (MB-Key) + 移動キー (Move-Key) とが与えられる。これにより、一般の再生装置でも、本発明にかかる再生装置でも再生が可能となる。

次に、本発明にかかる再生装置により、ディスクD1内のコンテンツデータを新たなディスクD2に移動する場合は、ディスクD1は、移動キー (Move-Key) を削除され媒体キー (MB-Key) のみを有するディスクD1' となる。新たなディスクD2には、移動キー (Move-Key) のみが記録される。これにより、ディスクD1' は、一般の再生装置で再生することだけが可能となる。又、ディスクD2は、一般の再生装置で再生することはできず、本発明に係る記録再生装置のみで再生したり移動処理を行うことができる。

更に、このような移動キー (Move-Key) となったディスクD2のコンテンツデータを、新たな光ディスクD3に移動する場合は、本発明にかかる再生装置により、光ディスクD2の移動キー (Move-Key) は、削除されて再生不能となる。光ディスクD3は、移動キー (Move-Key) のみが記録され、本発明にかかる記録再生装置のみにより再生したり移動処理を行うことができる。

又、更に、本発明に係る記録再生装置による光ディスクDのコンテンツデータの移動は、その対象を光ディスクだけに限るものではなく、SD (Secure Digital) カード等の一般的なデジタル記録媒体を対象とするものである。ここで、光

ディスクD3からSD (Secure Digital) カードD4への移動キー (Move-Key) の移動を行うことができ、先の光ディスクD2から光ディスクD3の移動の場合と同様に、光ディスクD3は、移動キー (Move-Key) を削除されて再生不能となり、SD (Secure Digital) カードD4は、移動キー (Move-Key) のみが記録されて、本発明にかかる記録再生装置のみにより再生したり移動処理を行うことができる。

＜本発明に係るコンテンツ管理方法の適用例＞

次に、本発明に係るコンテンツ管理方法を、具体的な光ディスク記録再生装置に適用した場合の実施形態について、図面を用いて詳細に説明する。図6は、本発明に係るコンテンツ管理方法を適用した記録再生装置の構造の一例を示すブロック図、図7は、記録再生装置に適用した場合の暗号化方法の詳細の一例を説明するブロック図、図8は、復号方法の詳細の一例を説明するブロック図である。

【0024】

(記録再生装置)

本発明に係るコンテンツ管理方法が適用される光ディスク記録再生装置Aを図6に上げており、光ディスク記録再生装置Aは、全体の動作を司るシステム制御部162と、作業エリアとなるRAM161と、ROM160と、サーボ制御部152とによる制御部を有する。更に、光ディスクDにレーザ光を照射する光ピックアップ154と、ここからの再生のための検出信号を受け、又、記録のための信号を供給し、ECC処理等を行う信号処理部156とを有しており、図1等に上述したバス認証部21を有し、更に、ケーブルを介して、同様にバス認証部21を有しエンコード・デコード等を行うデータ処理部158を有している。又、信号処理部156には、SDカード等の記録媒体のインターフェースであるメディアリーダーライター166が接続されている。又、データ処理部158には、RAM159、外部装置との信号の入出力を行うインターフェース165が接続されている。

又、更に、上記のサーボ制御部152に接続されるサーボ制御系各処理回路155と、これに接続されるアクチュエータドライバ153と、ディスクモータ151とを有している。

【0025】

このような構成を有する光ディスク装置Aにおいて、システム制御部162はRAM161を作業エリアとして使用し、ROM160に記録された本発明を含むプログラムに従って所定の動作を行う。光ピックアップ154から出力されたレーザ光は、光ディスクDに照射される。光ディスクDからの反射光は、ヘッドアンプで電気信号に変えられる。この電気信号は、信号処理部156に入力される。信号処理部156には、RFアンプなどが含まれる。

【0026】

記録動作時は、図1を用いて詳述した暗号化処理がコンテンツデータに施されて、光ディスクDに記録処理がなされる。更に、詳しく述べると、データ処理部158が図示しないライトチャンネル回路で作られた書込みクロックを用いて、インタフェース165を通して送られてくるコンテンツデータに誤り検出符号（EDC）やIDを付加し、上述した暗号化によるデータスクランブル処理を施し、更に誤り訂正符号（ECC）を付加し、同期信号を付加し、併せて同期信号以外を変調し、対応メディアに最適なライトストラテジーにより制御されたレーザ光により光ディスクDに信号を記録するものである。

【0027】

再生動作時は、図2及び図3を用いて詳述した復号処理がコンテンツデータに施されて、光ディスクDに格納されたコンテンツデータの再生処理が行われる。更に、詳しく述べると、光ピックアップ154のヘッドアンプから読出されたRF信号は、最適イコライザを通して、信号処理部156内の図示しないPLL回路に送られる。PLL回路で作られた読出しクロックでチャンネルデータが読み取られる。読み取られたデータは、上述した復号による復号処理が施され、更に、データ処理部158で同期化され、シンボルデータが読出される。その後誤り訂正や上述した復号処理によるデスクランブル処理が行われ、インタフェース165を通して外部に転送される。

【0028】

このようにして、上述した光ディスク記録再生装置Aにより、記録処理及び再生処理が施されるものである。

【 0 0 2 9 】

又、信号処理部 1 5 6 とデータ処理部 1 5 8 とは、バス認証部 2 1 をそれぞれ有しており、両者を結ぶケーブルのコネクタを外して信号を抽出し、不正コピーを行おうとする第三者への対策を行っている。すなわち、各バス認証部 2 1 はそれぞれ図示しない乱数発生器を有しており、これにより同一の暗号鍵を発生し、送信情報を暗号化した上で相手側に送信している。送信情報を受信した相手側の機器では、自分で発生した同一の暗号鍵により暗号化された送信情報を復号する。この暗号鍵は、所定時間に応じて変化して発生しているものなので、第三者がこれを再現することは非常に困難であり、そのときの暗号鍵を再現することができない限り、ケーブルのコネクタを外して信号を抽出しても、コンテンツデータ等を不正コピーすることはできないこととなる。

【 0 0 3 0 】

(変調・復調処理による暗号鍵の秘匿)

ここで、信号処理回路 1 5 6 で行われている変調・復調回路の動作を応用した暗号鍵情報の秘匿処理について以下に述べる。なお、図 7 が示す記録処理のためのコンテンツ管理方法の要部において、A V エンコーダモジュール M 1 は、図 1 に示した A V エンコーダモジュール M 1 と同等のものであり、図 8 が示す記録処理のためのコンテンツ管理方法の要部において、A V デコーダモジュール M 2 は、図 3 に示した A V デコーダモジュール M 2 と同等のものであるので、ここでは説明を省略する。

【 0 0 3 1 】

図 7 のドライブ部 V 3 においては、図 1 のドライブ部 V 1 の構成に加えて、E C C 回路等が示されている。すなわち、メインデータであるコンテンツスクランブル 1 4 からの信号が E C C 回路 4 3 により誤り訂正符号が付加され、変調回路 4 4 で変調される。更に、暗号化した秘匿鍵 (E n c - M M) も、E C C 回路 4 7 により誤り訂正符号化し、第 2 変調回路 4 8 により変調され、セレクタ 4 5 により、メインデータの一部と置換した上で、ライトチャネル回路 4 6 により、光ディスク D の記憶領域に記録される。

一方、図 8 のドライブ部 V 4 においては、誤り訂正符号が付加されたデータを

光ディスクDから読み出し、第2復調回路45で復調し、ECC回路46により、暗号化秘匿鍵（E n c - M M）を抽出することができる。一方、図7において、メインデータの変調器44とは異なる第2変調器48を使って暗号化秘匿鍵（E n c - M M）を変調して記録されているので、読み出し部のメインデータの変調器42では、暗号化秘匿鍵（E n c - M M）を復調することができず、エラーデータとして処理される。これにより、第三者が不正コピーを目的に、暗号化秘匿鍵（E n c - M M）を抽出することができない。このように変調・復調処理を応用することで、通常のメインデータ復調処理では検出できない秘匿情報を作り出すことができ、暗号化鍵情報（E n c - M M）を実質的に秘匿領域に記録し再生したことと同等の処理を行うことができる。これにより、光ディスクのような受動的な記録媒体であっても、高度な保護システムを構築することが可能となる。

【0032】

（移動フローチャート1）

次に、先に簡単に説明したコンテンツデータの記録媒体間の移動処理について、フローチャートを用いて詳細に説明する。図9は、本発明に係るコンテンツ管理方法により暗号化されたコンテンツと鍵情報とを記録媒体D1に記録する動作を示すフローチャート、図10は、記録媒体D1から、他の記録媒体D2へコンテンツを移動する場合の動作を示すフローチャート、図11は、記録媒体D2から、他の記録媒体D3へコンテンツを移動する場合の動作を示すフローチャート、図12は、この移動を、チャンネルダウンを伴って行う場合の動作を示すフローチャートである。

【0033】

本発明に係るコンテンツ管理方法は、上述したように光ディスク記録再生装置の中の信号処理部156やデータ処理部158の構成により実現されるが、これらの処理は、検出情報にコンテンツ管理方法を施す手順を記述したプログラム等により実現されるものであっても可能である。以下、フローチャートを用いて、本発明に係るコンテンツ管理方法を詳細に説明する。

【0034】

図9が示すフローチャートにおいて、コピー制限されたコンテンツデータSから、光ディスクD等の記録媒体D1へと、コンテンツデータが複写される場合を説明する。

初めに、記録媒体D1から、鍵情報(MK)を生成するためのメディア鍵ブロック情報(MKB)と、メディア固有情報(M-ID)とを読み出し、これらをAVエンコーダ部M1へ転送する(S11)。そして、AVエンコーダ部M1にて、デバイス固有の復号鍵(DvK1)16で、メディア鍵ブロック情報(MKB)から鍵情報(MK)を抽出する。そして、鍵情報(MK)とメディア固有情報(M-ID)から、タイトル鍵暗号用の暗号鍵(MUK)を生成する(S12)。

【0035】

次に、タイトル鍵(TK)を乱数発生処理により生成する。そして、著作権保護が指定されたコンテンツデータを、タイトル鍵(TK)でスクランブル暗号化する(S13)。次に、タイトル鍵(TK)を、タイトル鍵暗号用の鍵(MUK)で暗号化し、暗号化されたタイトル鍵(Enc-TK)を生成する(S13)。次に、暗号化コンテンツ(Enc-Contents)と暗号化タイトル鍵(Enc-TK)をバス認証処理を経て、ドライブV1に転送する(S14)。

【0036】

ここで、記録コンテンツは移動許可されているかどうかを判断する(S15)。許可されていれば、乱数発生処理により秘匿鍵(MM)を生成する。そして、暗号化タイトル鍵(Enc-TK)を秘匿鍵(MM)で多重暗号化し、多重暗号化タイトル鍵(Enc2-TK)を生成する。そして、記録媒体D1に暗号化コンテンツ(Enc-Contents)及び暗号化タイトル鍵(Enc-TK)群の媒体キー(MB-Key)と、多重暗号化タイトル鍵(Enc2-TK)群の移動キー(Move-Key)を記録媒体D1へと記録する(S16)。

【0037】

更に、ドライブV1内のデバイス鍵(DvK2)でメディア鍵ブロック情報(MKB)より暗号鍵(MMK)を検出する。秘匿鍵(MM)を暗号鍵(MMK)で暗号化し、暗号化暗号鍵(Enc-MM)を生成する(S17)。そして、暗

号化暗号鍵 (E n c - M M) 信号を、秘匿領域に記録する (S 1 8)。

【 0 0 3 8 】

又、ステップ S 1 5 で許可されていなければ、記録媒体 D 1 に、暗号化コンテンツ (E n c - C o n t e n t s) と暗号化タイトル鍵 (E n c - T K) 群の媒体キー (M B - K e y) を記録する (S 1 9)。

【 0 0 3 9 】

これらの処理により、コンテンツデータが暗号化され、本発明に係るコンテンツ管理方法の特徴である、移動キー (M o v e - K e y ; E n c 2 - T K) と媒体キー (M B - K e y ; E n c - T K) との両方 (又は媒体キーのみ) が、光ディスク D 1 へと記録されるものである。

【 0 0 4 0 】

(移動フローチャート 2)

図 1 0 が示すフローチャートにおいて、記録媒体 D 1 から、他の記録媒体 D 2 へコンテンツを移動する場合の動作を説明する。

最初に、移動先記録媒体 D 2 から、メディア鍵ブロック情報 (M K B) と、メディア固有情報 (M - I D) とを読み出し、これらから暗号鍵 (M U K 2) を生成する (S 2 1)。次に、記録媒体 D 1 をセットし、コンテンツ管理情報を検出する (S 2 2)。ここで、対応コンテンツの媒体キー (M B - K e y) と移動キー (M o v e - K e y) があるかどうかを判断する (S 2 3)。

【 0 0 4 1 】

ステップ S 2 3 で、移動キー (M o v e - K e y) のみあると判断されれば、メディア鍵ブロック情報 (M K B) とデバイス鍵 (D v K 2) で暗号鍵 (M M K) を検出し、暗号化暗号鍵 (E n c - M M) を復号して秘匿鍵 (M M) を検出し、多重暗号化タイトル鍵 (E n c 2 - T K 2) を秘匿鍵 (M M) で復号して、暗号化タイトル鍵 (E n c - T K) を生成する (S 3 1)。

【 0 0 4 2 】

ステップ S 2 3 で、媒体キー (M B - K e y) と移動キー (M o v e - K e y) の両方があれば、バス認証を通して、記録媒体 D 1 のメディア鍵ブロック情報 (M K B) とメディア固有情報 (M - I D) を転送し、デバイス固有の復号鍵 (

D v K 1) で暗号鍵 (M U K) を検出する (S 2 4)。更に、暗号化タイトル鍵 (E n c - T K) を暗号鍵 (M U K) で復号し、タイトル鍵 (T K) を生成する。更に、記録媒体 D 1 から暗号化コンテンツを読み出し、タイトル鍵 (T K) で復号し、新しい乱数発生器で生成したタイトル鍵 (T K 2) にて、再スクランブル (暗号化) し、一時記録する (S 2 5)。そして、記録媒体 D 1 の対応コンテンツの移動キー (M o v e - K e y) である、多重暗号化タイトル鍵 (E n c 2 - T K) を消去する (S 2 6)。

【 0 0 4 3 】

次に、記録媒体を記録媒体 D 2 へ変更し、タイトル鍵 (T K 2) を暗号鍵 (M U K 2) で暗号化して、暗号化タイトル鍵 (E n c - T K 2) を生成する (S 2 7)。そして、記録ドライブ内の新たな秘匿鍵 (M M 2) を生成し、暗号化タイトル鍵 (E n c - T K 2) を多重暗号化して多重暗号化タイトル鍵 (E n c 2 - T K 2) を生成する。

【 0 0 4 4 】

そして、記録媒体 D 2 のメディア鍵ブロック情報 (M K B) とデバイス鍵 (D v K 2) で暗号鍵 (M M K) を生成し、秘匿鍵 (M M 2) を暗号化して暗号化暗号鍵 (E n c - M M 2) を生成する (S 2 8)。次に、タイトル鍵 (T K 2) で暗号化された暗号化コンテンツ (E n c - C o n t e n t s) と多重暗号化タイトル鍵 (E n c 2 - T K 2) を記録媒体 D 2 に記録する。更に、暗号化暗号鍵 (E n c - M M 2) を秘匿領域に記録する (S 2 9)。

【 0 0 4 5 】

又、ステップ S 2 3 で、移動キー (M o v e - K e y) 無しとなれば、移動不許可とする (S 3 0)。

【 0 0 4 6 】

これにより、移動元の記録媒体 D 1 は、移動キー (M o v e - K e y) を削除され、媒体キー (M B - K e y) だけとなり、コンテンツデータの移動が不可となり、従来の汎用機である再生装置で再生できるが移動不可の状態となる。一方、移動先の記録媒体 D 2 は、移動キー (M o v e - K e y) のみとなり、本発明に係るコンテンツ管理方法が可能な専用機のみで再生及びそれ以上の移動が可能

な状態となる。

(移動フローチャート 3)

図 1 1 が示すフローチャートにおいて、記録媒体 D 2 から、他の記録媒体 D 3 へコンテンツを移動する場合の動作を説明する。

初めに、移動先記録媒体 D 3 から、メディア鍵ブロック情報 (MKB) とメディア固有情報 (M-ID) を読み出し、暗号鍵 (MUK 2) を生成する (S 2 1)。次に、記録媒体 D 2 をセットし、コンテンツ管理情報を検出する (S 2 2)。そして、対応コンテンツの媒体キー (MB-Key) と移動キー (Move-Key) があるかどうか判断される (S 2 3)。

【0047】

移動キー (Move-Key) が無しとなれば、コンテンツデータは、移動不許可となる (S 3 0)。

【0048】

移動キー (Move-Key) のみあると判断されれば、メディア鍵ブロック情報 (MKB) とデバイス鍵 (DvK 2) とで暗号鍵 (MMK) を抽出する。そして、暗号化暗号鍵 (Enc-MM) を復号して秘匿鍵 (MM) を検出し、多重暗号化タイトル鍵 (Enc 2-TK 2) を秘匿鍵 (MM) で復号して、暗号化タイトル鍵 (Enc-TK 2) を生成する (S 3 1)。

【0049】

ステップ S 2 3 で、媒体キー (MB-Key) と移動キー (Move-Key) があると判断されれば、バス認証を通して、記録媒体 D 2 のメディア鍵ブロック情報 (MKB) と、メディア固有情報 (M-ID) を転送し、デバイス固有の復号鍵 (DvK 1) でタイトル鍵の暗号鍵 (MUK 2) が検出される (S 4 2)。次に、暗号化タイトル鍵 (Enc-TK) をタイトル鍵の暗号鍵 (MUK 2) で復号し、タイトル鍵 (TK 2) を検出する。そして、記録媒体 D 2 から暗号化コンテンツ (Enc-Contents) を読出し、一時記憶する (S 4 3)。そして、記録媒体 D 2 の対応コンテンツの移動キー (Move-Key) である、多重暗号化タイトル鍵 (Enc 2-TK 2) を消去する (S 2 6)。

【0050】

次に、記録媒体を記録媒体D3に変更し、タイトル鍵(TK2)を暗号鍵(MUK2)で暗号化して、暗号化タイトル鍵(Enc-TK3)を生成する(S27)。次に、記録ドライブ内の新たな秘匿鍵(MM3)を生成し、暗号化タイトル鍵(Enc-TK3)を多重暗号化して、多重暗号化タイトル鍵(Enc2-TK3)を生成する。そして、記録媒体D3のメディア鍵ブロック情報(MKB)とデバイス鍵(DvK2)とで暗号鍵(MMK)を生成し、秘匿鍵(MM3)を暗号化して暗号化暗号鍵(Enc-MM3)を生成する(S28)。そして、タイトル鍵(TK2)で暗号化された暗号化コンテンツ(Enc-Contents)と多重暗号化タイトル鍵(Enc2-TK3)を記録媒体D3に記録し、暗号化暗号鍵(Enc-MM3)をその秘匿領域に記録する(S29)。尚、図11のフローチャート3における暗号化タイトル鍵(Enc-TK3)は、図10のフローチャート2と共通する工程を多く含んでいるが、ステップS42とS43において、タイトル鍵(TK2)を暗号鍵(MUK2)で暗号化して暗号化タイトル鍵(Enc-TK3)が生成されている点が異なる。

【0051】

これにより、移動元の記録媒体D2は、移動キー(Move-Key)を削除され、コンテンツデータの移動や再生が不可能となる。一方、移動先の記録媒体D3は、移動キー(Move-Key)のみとなり、本発明に係るコンテンツ管理方法が可能な専用機のみで再生及びそれ以上の移動が可能な状態となる。

又、本発明に係るコンテンツ管理方法が対象とする記録媒体は、光ディスクだけではなく、図5に示すように、SD(Secure Digital)カードD4等の一般的なデジタル記録媒体を対象とすることができる。

【0052】

(移動フローチャート4)

更に、図11のフローチャートで示すコンテンツデータの移動処理において、マルチチャネルのオーディオソースデータ(5.1チャンネル)を2チャンネルにチャンネルダウンして処理する場合を説明する。これらの処理は、基本的に図11のフローチャートで示した処理と同等であるが、図11のフローチャートのステップS42及びステップS43が、ステップS44と置き代わる処理により行わ

れる。

すなわち、図 1 2 のフローチャートのステップ S 4 4 において、暗号化されたタイトル鍵 (E n c - T K) を暗号鍵 (M U K 2) により復号し、タイトル鍵 (T K 2) を生成する。そして、記録媒体 D 2 から暗号化コンテンツ (E n c - C o n t e n t s) を読み出し、タイトル鍵 (T K 2) で復号する。更に、マルチチャネルのオーディオソースデータを 2 チャネルにチャンネルダウンし、乱数発生器で生成したタイトル鍵 (T K 3) にて再度スクランブル (暗号化) し、一時記録する (S 4 4)。

【 0 0 5 3 】

このような処理において、オーディオソースデータ (5. 1 チャネル) を 2 チャネルにチャンネルダウンしながら、コンテンツデータを、記録媒体 D 2 から新たな記録媒体 D 3 へと移動でき、その作用効果は、図 1 1 のフローチャートの移動処理と同等のものである。

【 0 0 5 4 】

(曲ファイルごとの鍵情報と鍵の増殖方法)

又、更に、本発明に係るコンテンツ管理方法が対象とするコンテンツデータは、例えば、複数曲の音楽情報としての複数の音声ファイルという形態をとることが可能である。複数の情報は例えば映像ファイルや画像ファイルでもかまわないが、以下、音声ファイルに例をとって説明する。この形態においては、図 1 に示される乱数発生器 1 8 が供給するタイトル鍵 (T K) も、この複数ファイルごとに一つ一つ異なるものを設け、それぞれ暗号化することで、音楽情報の 1 曲ごとの他の記録媒体への移動が可能となる。これにより、ユーザのコンテンツ利用の自由度を非常に向上させることができる。

しかしながら、複数のタイトル鍵 (T K) に一つ一つ対応させて、移動キー (M o v e - K e y = E n c 2 - T K) を生成するとなると、ドライブ部 V 1 における秘匿鍵 (M M) を、複数の音楽ファイルの数だけ用意する必要が出てくる。しかし、曲の数だけ秘匿鍵 (M M) を用意して、これを全て光ディスク D の秘匿領域に格納すると、秘匿領域は大きな記憶容量が必要となり、記憶容量の増大を招くことから好ましくない。特に、上述した変調・復調処理を利用した秘匿情報

記録方式では、メインデータの一部を破壊して秘匿情報を記録することになりメインデータの再生処理に好ましくないため、できる限り秘匿情報の削減が望ましい。

【 0 0 5 5 】

そこで、秘匿鍵（MM）を元に、一定の手順で複数の鍵を増殖させてこれを暗号化に用い、秘匿領域に格納するのは増殖の元となった秘匿鍵（MM）のみとすることで、秘匿領域の記憶容量を削減しながら、複数のファイルをそれぞれ管理することが可能となる。

図 1 3 は、本発明に係るコンテンツ管理方法における秘匿鍵（MM）の生成方法を示す図であり、この図において、図 1 の乱数発生器 2 4 等において、乱数 G 6 1 から生成される鍵元データ（MM）に基づく秘匿鍵（MM 1）が生成され、その後は、コンテンツデータの識別コード、又は、序列番号等で決められる回数で特定関数 K を乗算していくことで、新たな秘匿鍵（MM 2 ～ MM n）が生成される。この複数の秘匿鍵（MM 2 ～ MM n）を用いて、複数の暗号化されたタイトル鍵（Enc-TK 1 ～ Enc-TK n）6 3 - 1 ～ n をそれぞれ暗号化 6 4 していく。

【 0 0 5 6 】

しかしながら、秘匿領域に格納するのは、鍵元データ（MM）を暗号化した暗号化暗号鍵（Enc-MM）のみでよいので、必要な秘匿領域の記憶容量は増大することが無いため、多くの複数ファイルについて、高いセキュリティを伴ってコンテンツ管理を行うことが可能となる。

（管理情報）

本発明に係るコンテンツ管理方法においては、移動キー（Move-Key）と媒体キー（MB-Key）とにより、コンテンツデータの再生や移動が管理されるため、これらの暗号鍵ファイルは、暗号化コンテンツと同等に重要なデータである。すなわち、暗号化暗号鍵が復号できないと、暗号化コンテンツも復号や再生を行うことができない。そこで、図 1 4 に示すように、記録媒体（例えば光ディスク）のデータエリアに、移動キー（Move-Key）ファイルと媒体キー（MB-Key）ファイルとがそれぞれ異なるファイル領域に設けられている

。そして、各 ECC ブロックに 1 テーブルを配置し、各々、4 ECC ブロックに 4 重書きすることにより、データの信頼性を高めている。

【0057】

又、これらのファイルのテーブルを図 15 に示す。すなわち、記録メディアには、「媒体キー (MB-Key) と移動キー (Move-Key)」、「媒体キー (MB-Key) のみ」、「移動キー (Move-Key) のみ」の三種類が存在する。又、コンテンツファイル数が多い場合は個別管理から、夫々のコンテンツ暗号鍵に対して、媒体キー (MB-Key) と移動キー (Move-Key) の関係を容易に読み出せることが必要である。そこで、図 15 に示す移動キー (Move-Key) のテーブルと媒体キー (MB-Key) のテーブルでは、夫々の暗号化暗号鍵に対する関連の暗号鍵の有無情報や、図 13 で示した秘匿鍵 (MM) の生成方法が取られた場合の利用した情報を、情報の組としてテーブルが構成されている。このテーブルを一覧することで、それぞれのコンテンツデータについて、コンテンツ移動が可能かどうか等の判断を容易に行うことが可能となる。

以上記載した様々な実施形態により、当業者は本発明を実現することができるが、更にこれらの実施形態の様々な変形例を思いつくことが当業者によって容易であり、発明的な能力をもたなくとも様々な実施形態へと適用することが可能である。従って、本発明は、開示された原理と新規な特徴に矛盾しない広範な範囲に及ぶものであり、上述した実施形態に限定されるものではない。

【0058】

例えば、秘匿鍵が格納される秘匿領域は、上述した変調・復調処理を利用する際に、秘匿情報記録再生の領域は、メインデータとは別の記録再生エリアに対応させるものであってもよい。このような方法を取ることで、メインデータはエラー成分を加えられることはなくなるので、コンテンツデータの信頼性を損なうことがなくなる。

【0059】

【発明の効果】

以上詳述したように本発明によれば、コンテンツデータの移動を保証する移動

キー (Move-Key: Enc2-TK) と、従来の汎用機 (例えば光ディスク装置等) による再生装置でも再生することを保証する媒体キー (MB-Key: Enc-TK) とを暗号化コンテンツデータと共に記録媒体へと記録することにより、秘匿領域に格納された秘匿鍵を復号できる本発明に係る記録再生装置においては、移動キー (Move-Key) による再生や移動が可能であり、従来の汎用機である再生装置においては、媒体キー (MB-Key) による再生が保証される。これにより、コンテンツデータの拡散を防止しながらも専用機による移動処理が可能であると共に、従来機によるコンテンツデータの再生を行うことが可能となる。

【図面の簡単な説明】

【図 1】

本発明に係るコンテンツ管理方法による暗号化の一例を示すブロック図。

【図 2】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツの一般的な方法による復号の一例を示すブロック図。

【図 3】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツの本発明に係る方法による復号の一例を示すブロック図。

【図 4】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツを記録した記録媒体の一例。

【図 5】

本発明に係るコンテンツ管理方法による移動キー (Move-Key: Enc2-TK) と媒体キー (MB-Key: Enc-TK) の移動の一例を示す説明図。

【図 6】

本発明に係るコンテンツ管理方法を適用した記録再生装置の構造の一例を示すブロック図。

【図 7】

本発明に係るコンテンツ管理方法を記録再生装置に適用した場合の暗号化方法の詳細の一例を説明するブロック図。

【図 8】

本発明に係るコンテンツ管理方法を記録再生装置に適用した場合の復号方法の詳細の一例を説明するブロック図。

【図 9】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツと鍵情報とを記録媒体 D 1 に記録する動作を示すフローチャート。

【図 1 0】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツが記録された記録媒体 D 1 から、他の記録媒体 D 2 へコンテンツを移動する場合の動作を示すフローチャート。

【図 1 1】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツが記録された記録媒体 D 2 から、他の記録媒体 D 3 へコンテンツを移動する場合の動作を示すフローチャート。

【図 1 2】

本発明に係るコンテンツ管理方法により暗号化されたコンテンツが記録された記録媒体 D 2 から他の記録媒体 D 3 へのコンテンツの移動を、チャンネルダウンを伴って行う場合の動作を示すフローチャート。

【図 1 3】

本発明に係るコンテンツ管理方法における秘匿鍵 (MM) の生成方法を示す図。

【図 1 4】

本発明に係るコンテンツ管理方法における記録媒体中の移動キー (Move Key : Enc 2 - TK) と媒体キー (MB - Key : Enc - TK) の格納領域の一例を示す図。

【図 1 5】

本発明に係るコンテンツ管理方法における記録媒体中の移動キー (Move

Key : Enc 2 - TK) と媒体キー (MB - Key : Enc - TK) のテーブルの一例を示す図。

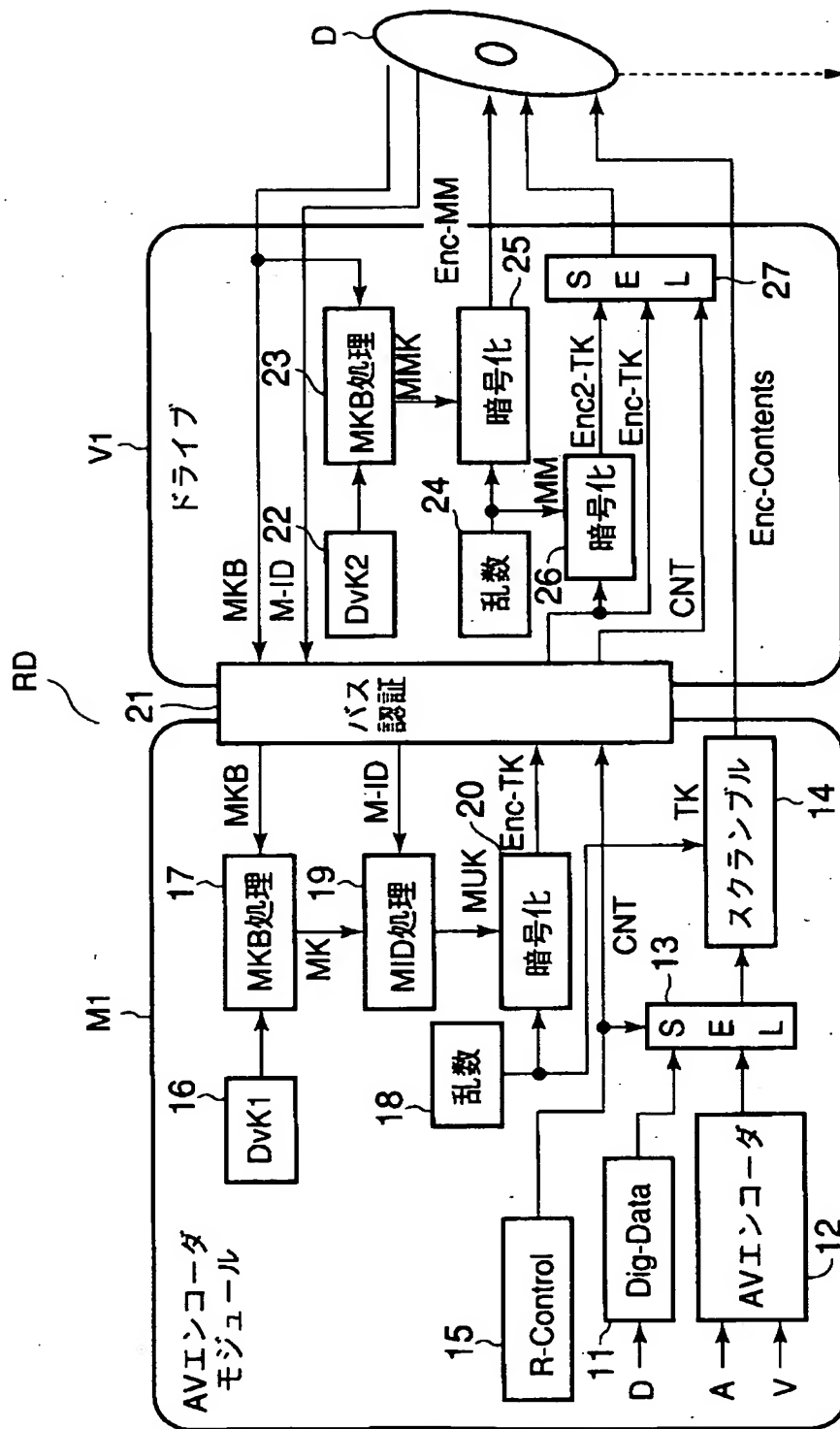
【符号の説明】

1 1 …デジタルデータ、 1 5 … R - Control (記録制御) , 1 6 …デバイス鍵、
1 7 …MKB 処理、 1 8 …乱数発生器、 1 9 …MID 処理、 2 0 …暗号化回路、
2 1 …バス認証部、 2 2 …デバイス鍵、 2 3 …MKB 処理、 2 4 …乱数発生器、
2 5 …暗号化回路、 2 6 …暗号化回路、 2 7 …セレクタ。

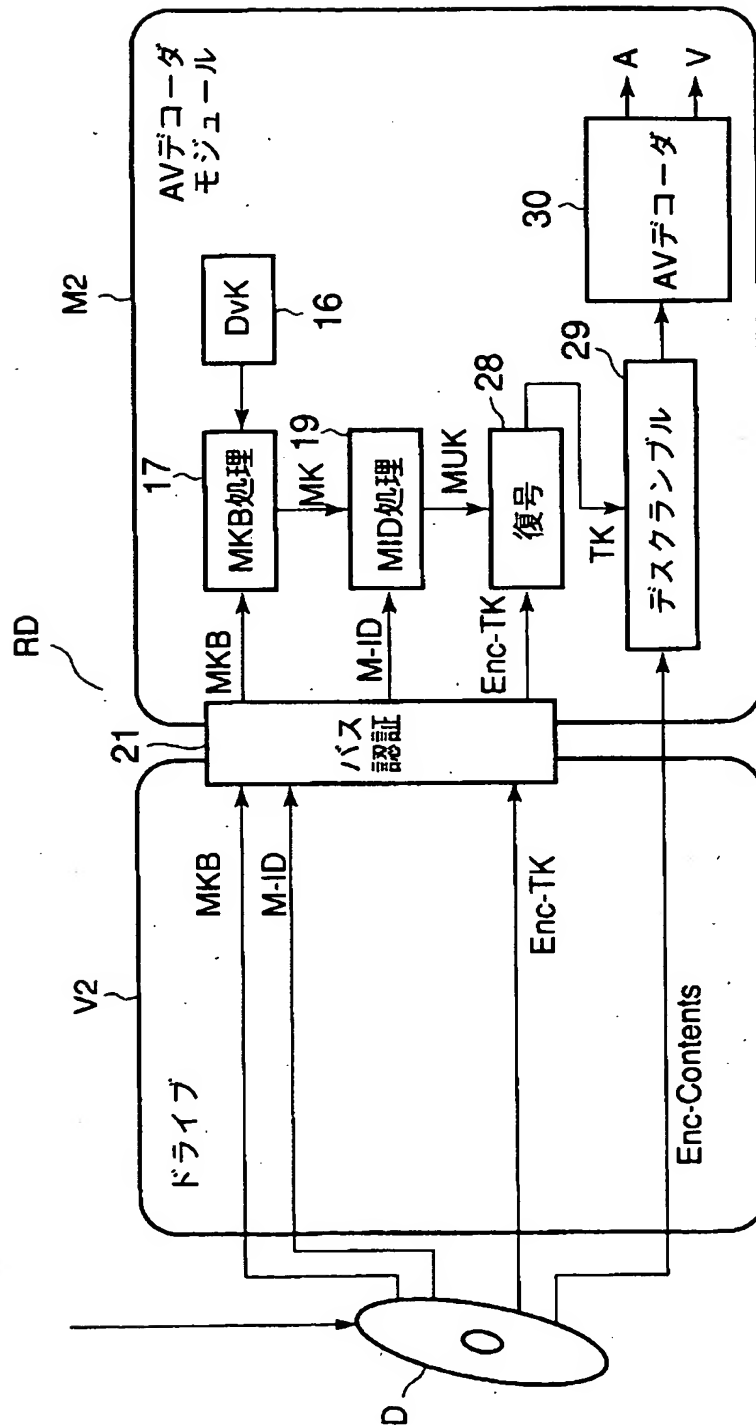
【書類名】

図面

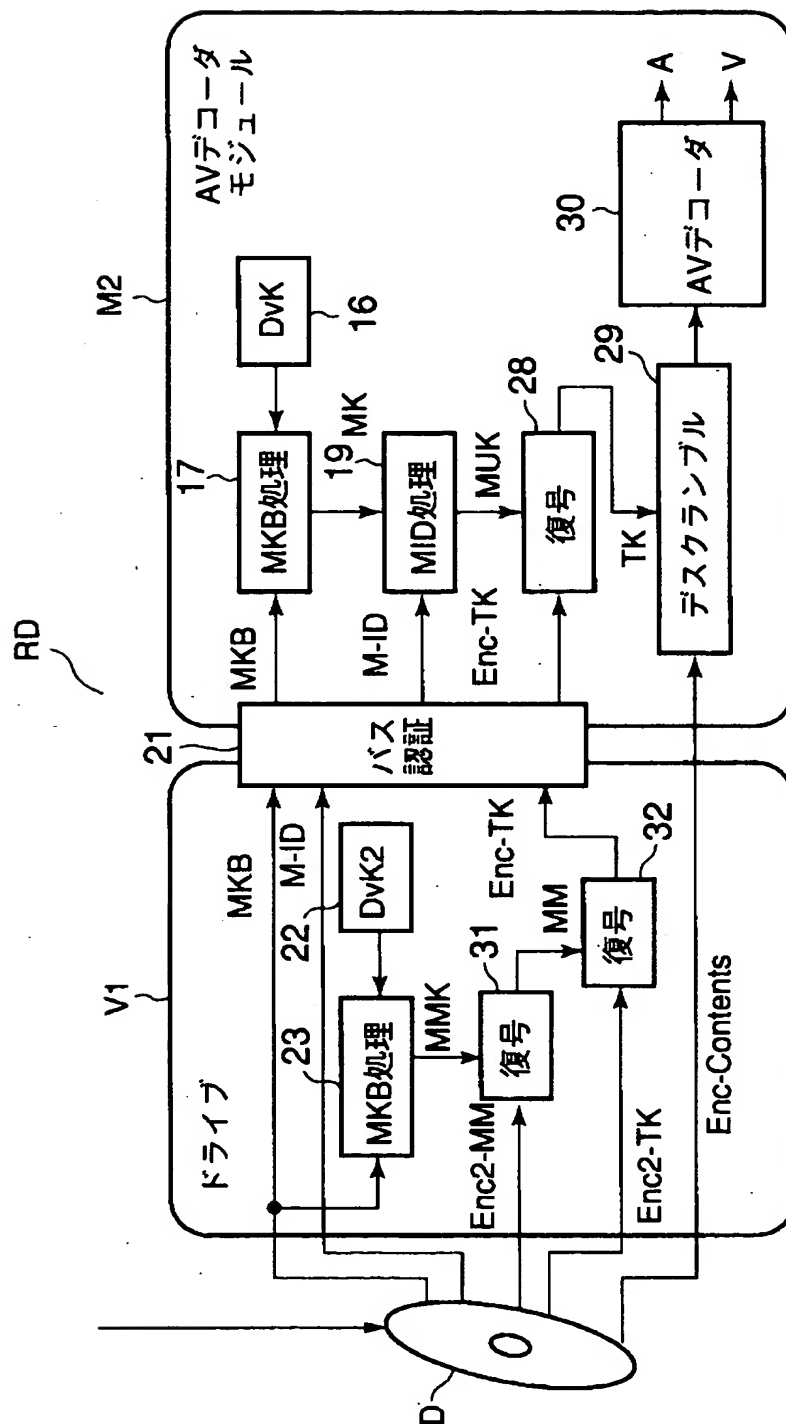
【図 1】



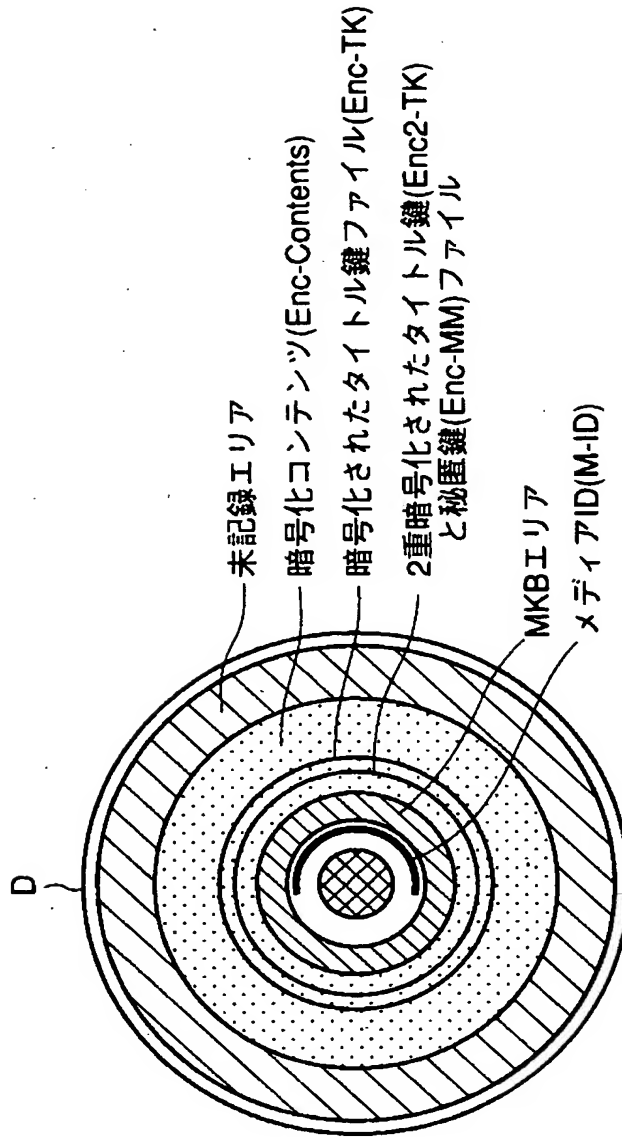
【図2】



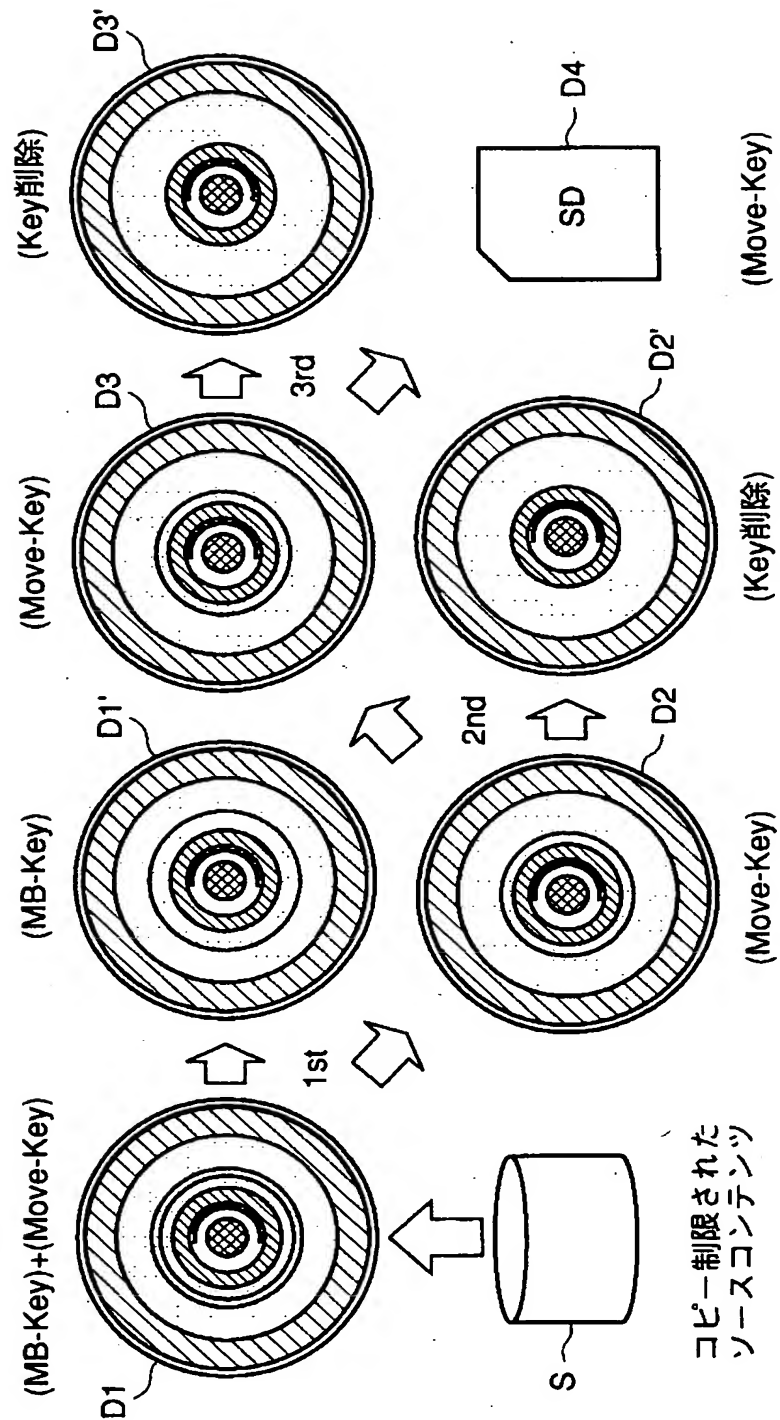
【図3】



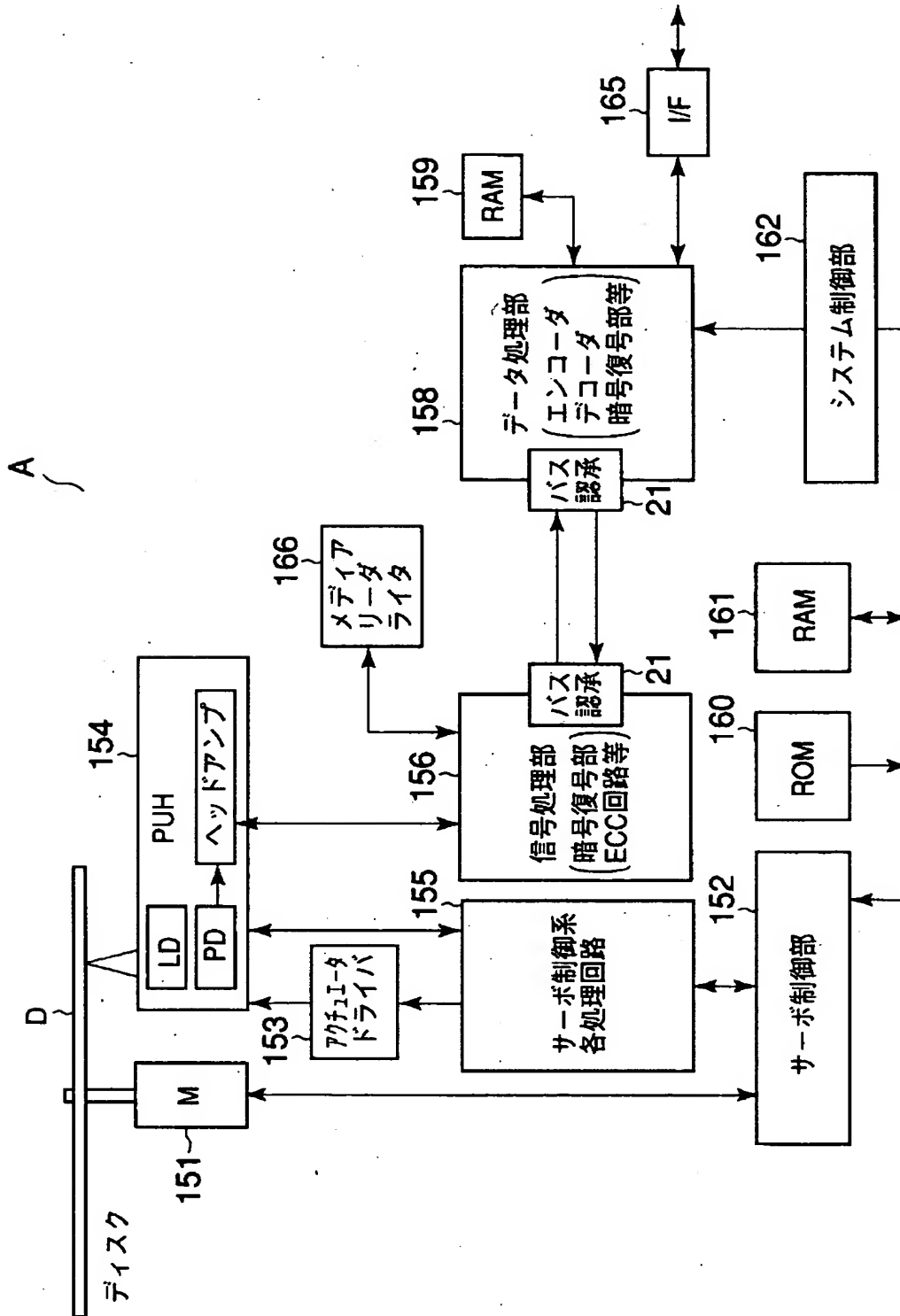
【図 4】



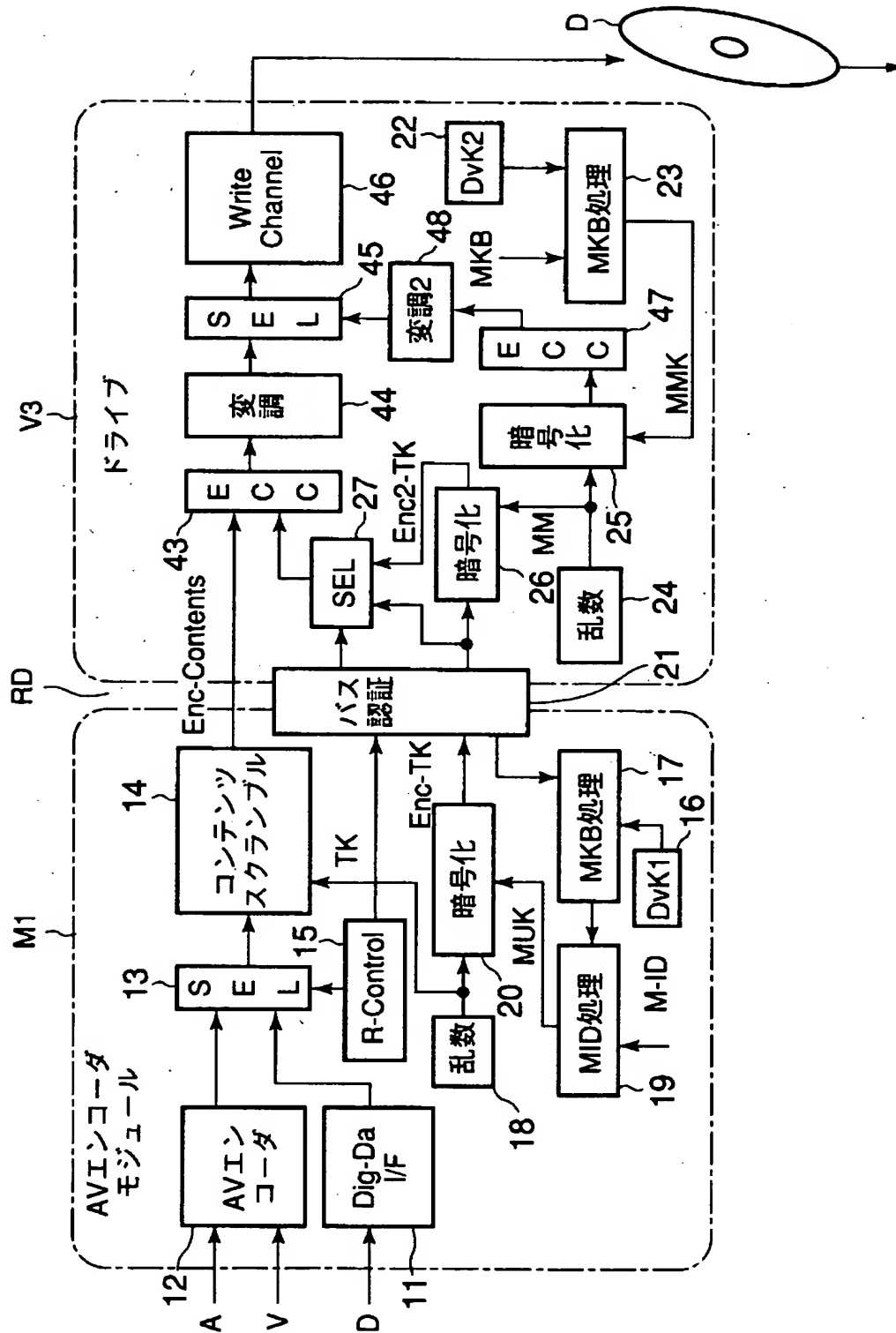
【図 5】



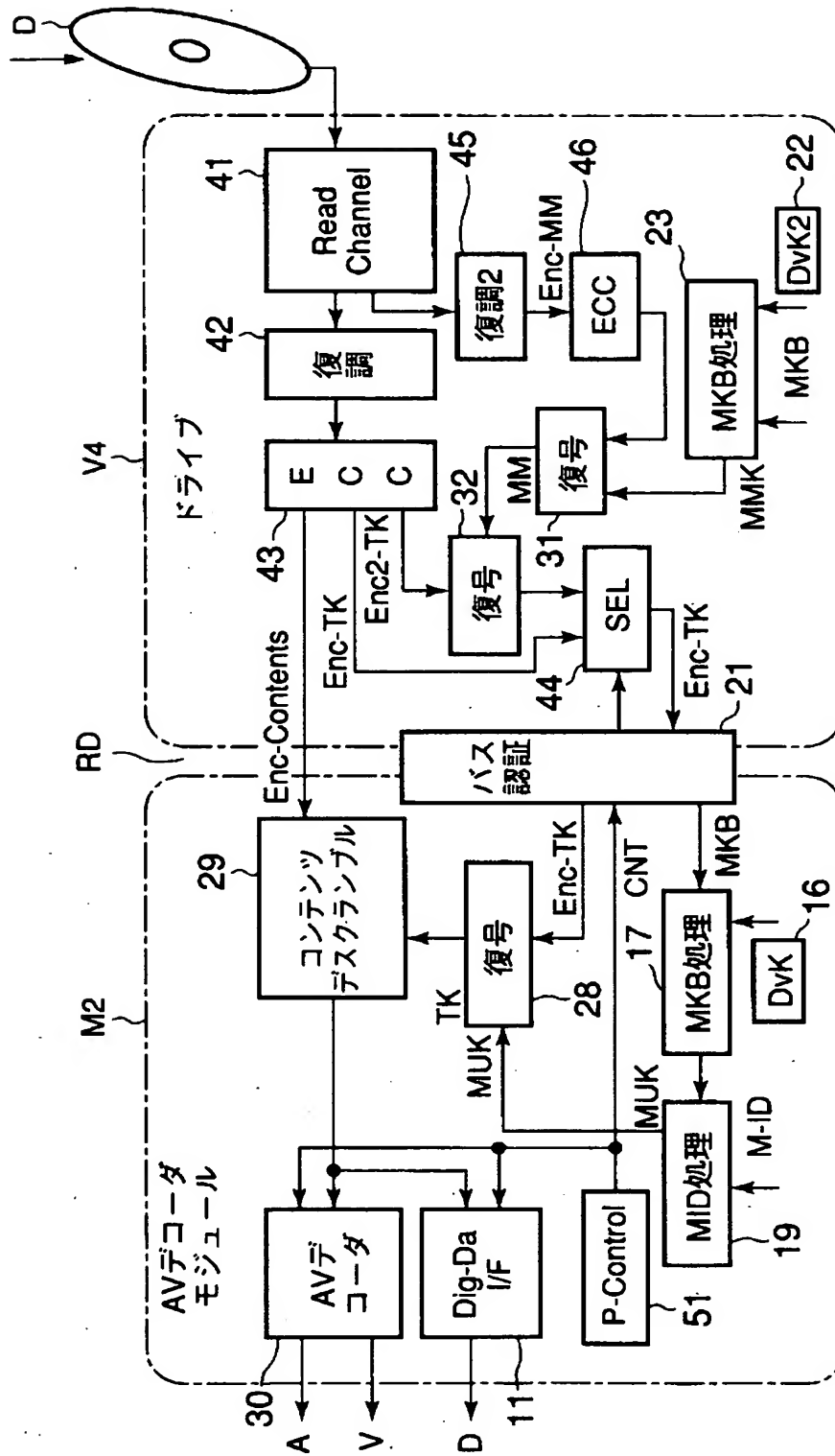
【図 6】



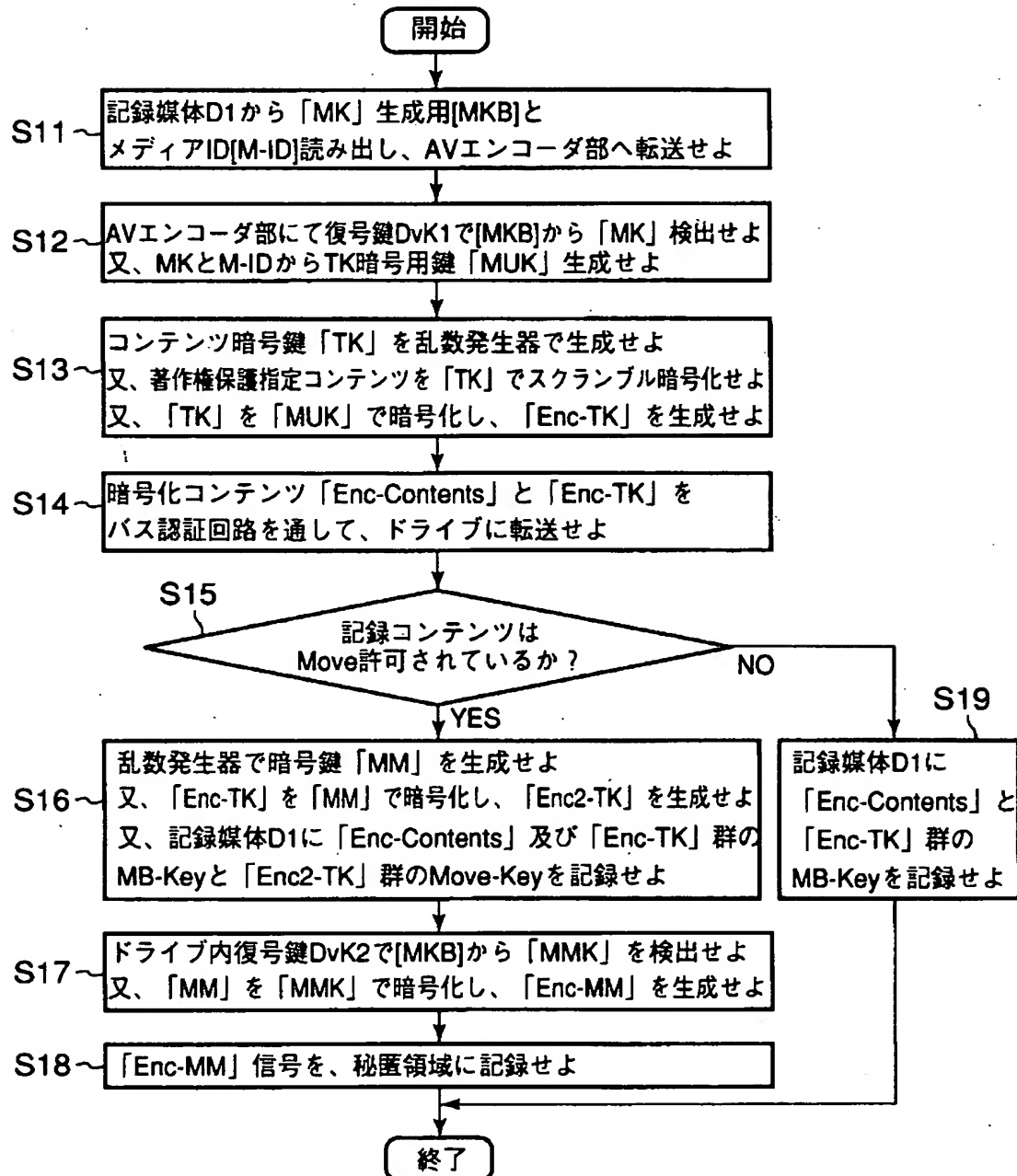
【圖 7】



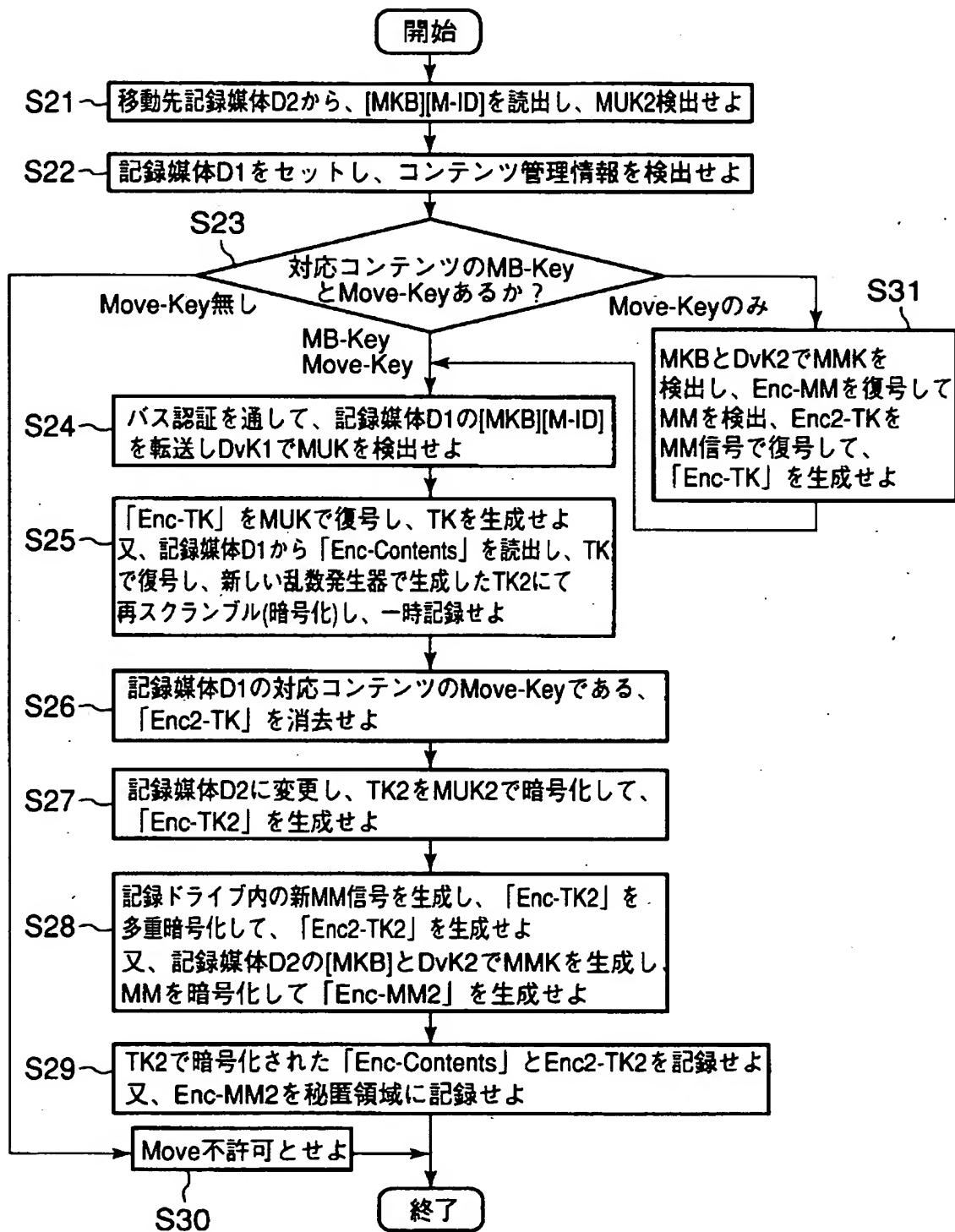
【図8】



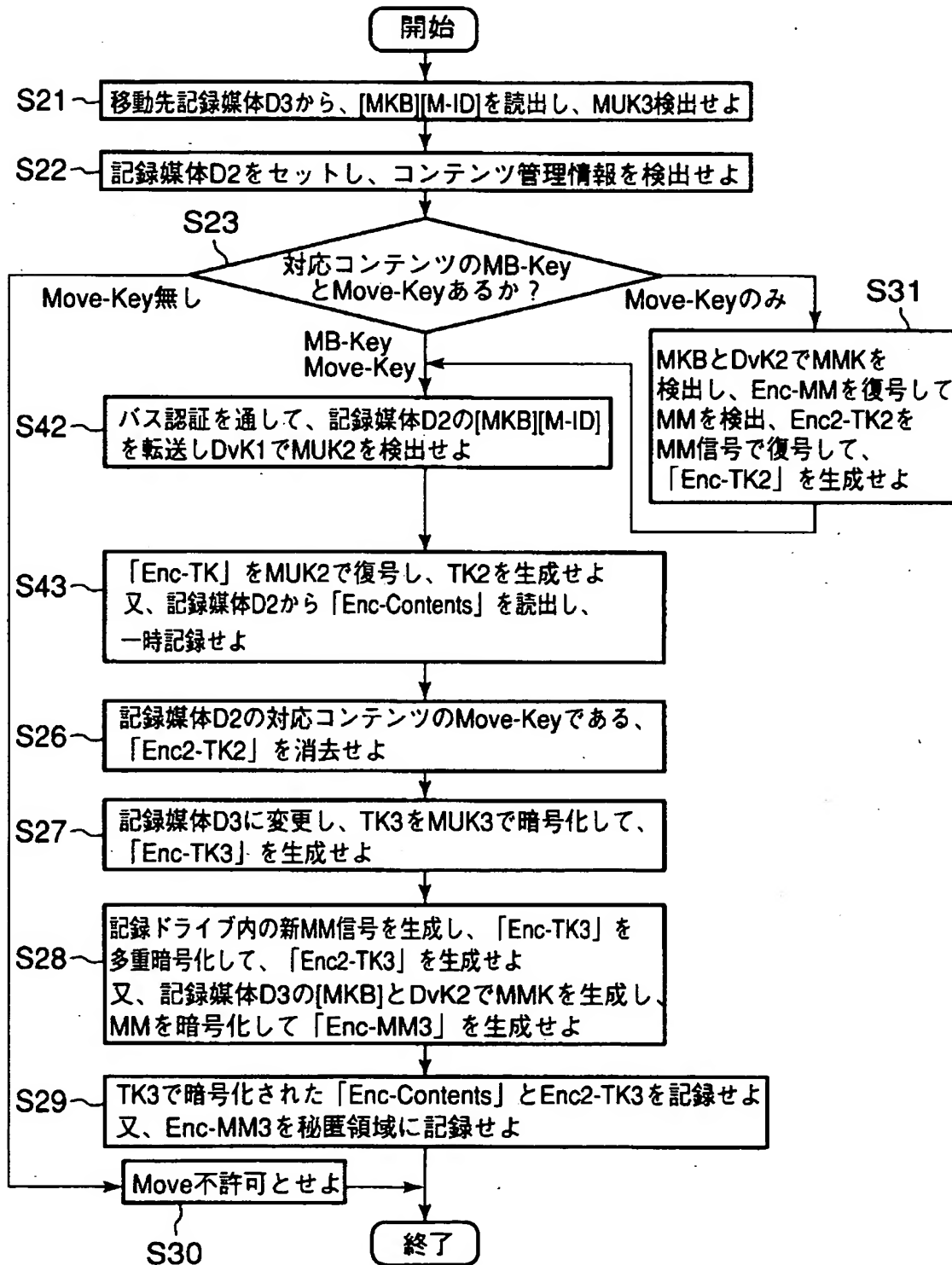
【図 9】



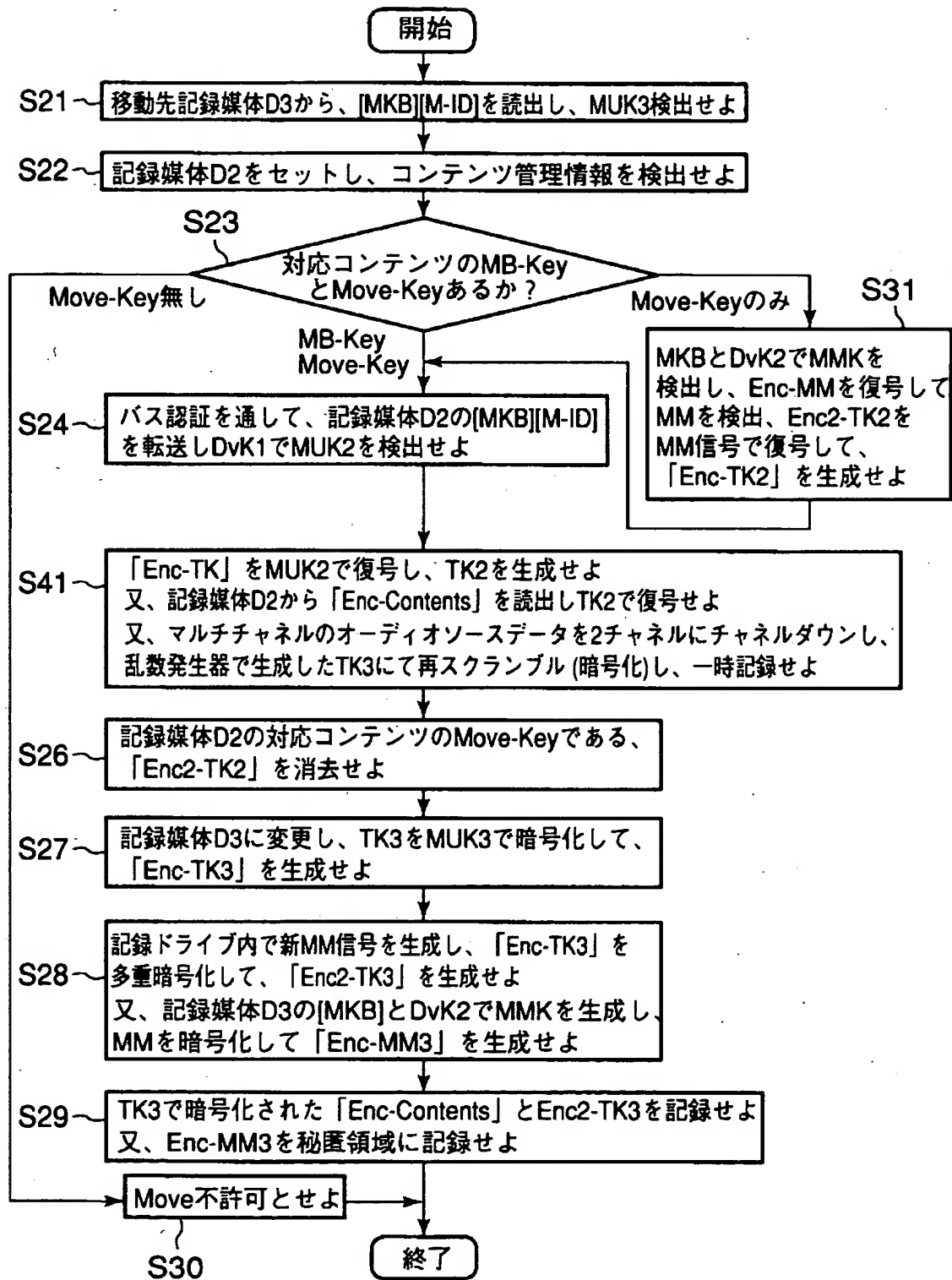
【図 1 0】



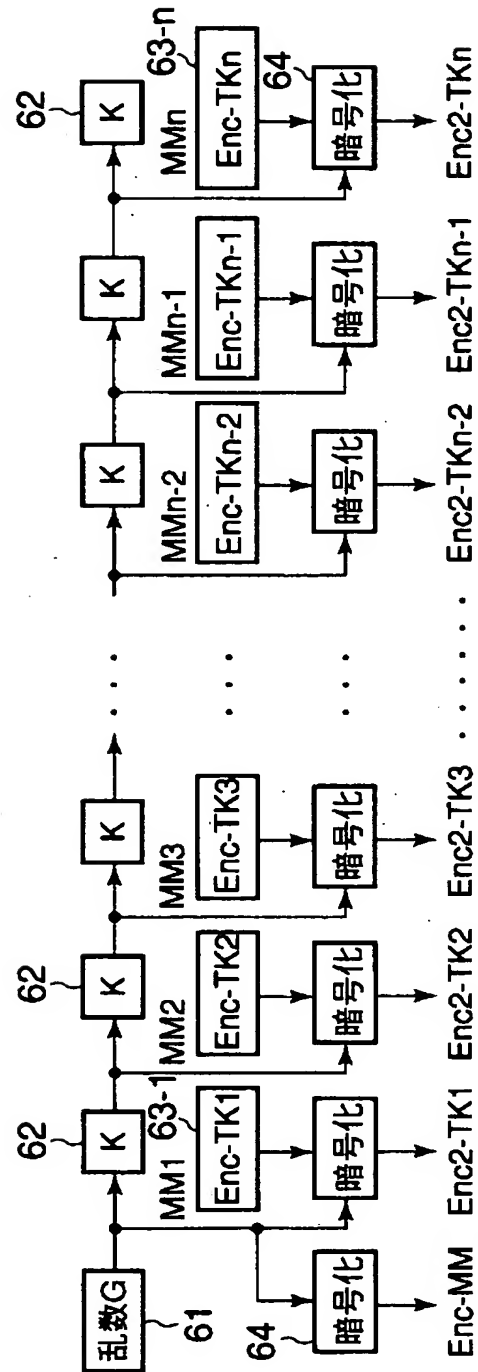
【図 1 1】



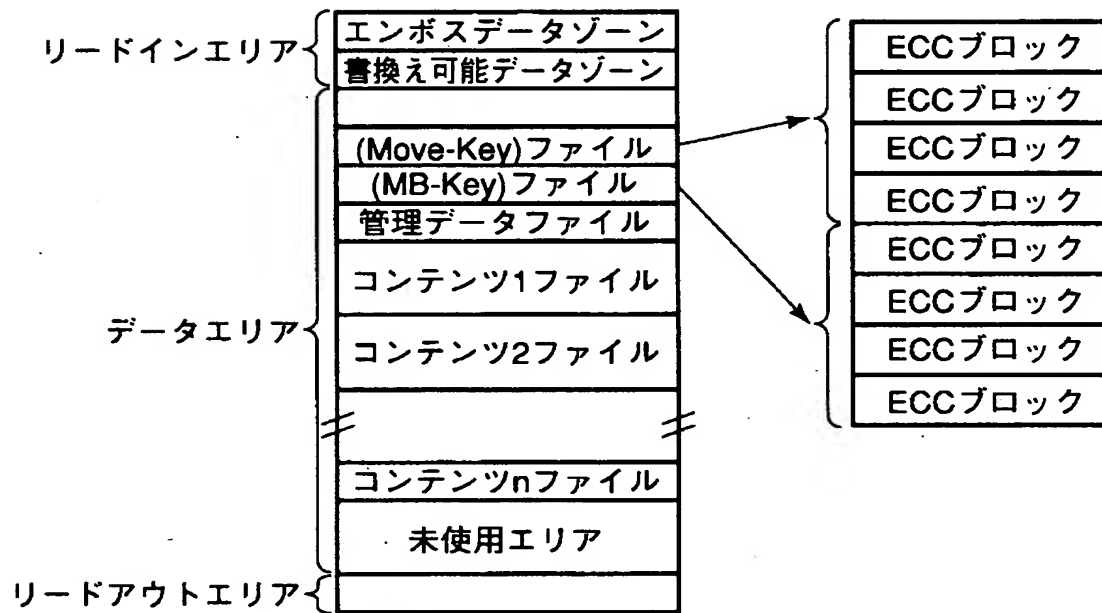
【図 1 2】



【図 13】



【図 1 4】



【図 1 5】

MB-Key の テーブル				Move-Key の テーブル			
暗号化暗号鍵のファイル識別(MB-Key)				暗号化暗号鍵のファイル識別(Move-Key)			
Cont 暗号化暗号鍵の数				Cont 暗号化暗号鍵の数			
Cont-1	Enc-TK	Cont-1 記録番号	○	Cont-1	Enc2-TK	Cont-1 記録番号	○
Cont-2	Enc-TK	Cont-2 記録番号	○	Cont-2	Enc2-TK	Cont-2 記録番号	○
Cont-3	Enc-TK	Cont-3 記録番号	X	-	-	Cont-3 記録番号	○
Cont-(n-1)	Enc-TK	Cont-(n-1) 記録番号	○	Cont-(n-1)	Enc2-TK	Cont-(n-1) 記録番号	○
Cont-n	Enc-TK	Cont-n 記録番号	○	Cont-n	Enc2-TK	Cont-n 記録番号	○
RSB	RSB	RSB		RSB	RSB	RSB	
RSB	RSB	RSB		RSB	RSB	RSB	

(a) Enc-2TKの有無情報

(b) Enc-TKの有無情報

(ECCブロックに1 テーブルを配置し、各々4ECCブロックに4重書き)

【書類名】 要約書

【要約】

【課題】 コンテンツの拡散を防止しつつコンテンツの移動を可能にし、更に、従来の汎用装置での一定の再生互換性も保証するコンテンツ管理方法。

【解決手段】 第1の鍵(TK)でコンテンツデータを暗号化し、第1の鍵を複数種類の第2の鍵(MUK)で暗号化し、暗号化された第1の鍵(Enc-TK)を第3の鍵(MM)で多重暗号化し、第3の鍵を第4の鍵(MMK)で暗号化し、これらの暗号化されたコンテンツデータ(Enc-Contents)と、第2の鍵で暗号化された第1の鍵(Enc-TK)である媒体キーと、第2・第3の鍵で多重暗号化された第1の鍵(Enc2-TK)である移動キーとを記録媒体に記録し、第4の鍵で暗号化された第3の鍵(Enc-MM)を秘匿領域に記録するコンテンツ管理方法であり、移動キーと媒体キーとにより管理される。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝
2. 変更年月日 2003年 5月 9日
[変更理由] 名称変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝